PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-141429
(43)Date of publication of application : 16.05.2003

(51)Int.Cl. G06F 17/60
G06K 17/00
G06K 19/00

(21)Application number : 2001-334967
(22)Date of filing : 31.10.2001

(71)Applicant : SONY CORP
(72)Inventor : FUKADA AKIRA
OSHIMA TAKUYA

(54) DATA TRANSFER SYSTEM AND METHODVALUE INFORMATION MOVING SERVICE DEVICE AND METHODAND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To securely move a plurality of pieces of value information between portable terminals.
SOLUTION: A server for moving the value securely moves a plurality of pieces of value information in an IC chip onto another IC chip while preventing the copying and falsifying of the value information without showing the value information itselfa key necessary for accessing the value information and its logic to devices excluding that having the authority by controlling a tamper- proof hardware module SAM in which the value information itselfthe key necessary for accessing the value information and its logic are sealed. For examplewhen the portable terminal is exchanged to a new modelall pieces of value information can be securely moved only by connecting the terminal to one part.

CLAIMS

[Claim(s)]
[Claim 1]A data transfer system characterized by comprising the following for moving value information.
A key for accessing the value information itself and value information used as a moved objectand a value information service device which holds the logic safely.
A value information move service device which relays upload to said value information

service device of value information stored in an information recording medium of a moved materialand download of value information from said value information service device to an information recording medium of a movement destination.

[Claim 2]After said value information move service device's changing a key for accessing value information on an information recording medium of a moved material into **** from this key at the time of normal usewhile uploading value information to said value information service deviceThe data transfer system according to claim 1 characterized by what is changed into this key from **** after downloading value information from said value information service device on an information recording medium to a movement destination.
[Claim 3]When there are two or more keys for two or more value information being held on an information recording medium of a moved materialand accessing each value information itself and value information and value information service devices which hold the logic safelyThe data transfer system according to claim 1 characterized by what said value information move service device performs upload of value information from an information recording medium of a moved materialand download to an information recording medium of a movement destination for for every value information service device.
[Claim 4]The data transfer system according to claim 1 characterized by what initialization processing of an information recording medium of a movement destination is performed for before said value information move service device downloads value information from a value information service device.
[Claim 5]The data transfer system according to claim 1 characterized by what said value information move service device does for the authenticating processing of an information recording medium of a moved materialand/or the information recording medium of a movement destination.
[Claim 6]A data transfer method characterized by comprising the following for moving value information.
A step which relays upload of a key for accessing the value information itself and value informationand value information to a value information service device which holds the logic safely from an information recording medium of a moved material.
A step which stores temporarily value information which a value information service device is movingand a step which relays download of value information from said value information service device to an information recording medium of a movement destination.

[Claim 7]A step which changes a key for accessing value information on an information recording medium of a moved material into **** from this key at the time of normal use before relaying upload to a value information service deviceThe data transfer method according to claim 6 having further a step changed into this key from

**** after downloading value information from a value information service device on an information recording medium to a movement destination.
[Claim 8]When there are two or more keys for two or more value information being held on an information recording medium of a moved materialand accessing each value information itself and value information and value information service devices which hold the logic safelyThe data transfer method according to claim 6 characterized by what a step which relays a step which relays said uploadand/or said download is performed for for every value information service device.
[Claim 9]The data transfer method according to claim 6 characterized by what it has further for a step which performs initialization processing of an information recording medium of a movement destination before downloading value information from a value information service device.
[Claim 10]The data transfer method according to claim 6 characterized by what it has further for a step which carries out authenticating processing of an information recording medium of a moved materialand/or the information recording medium of a movement destination.
[Claim 11]A value information move service device which serves movement of value information between information recording mediacomprising:
A means to relay upload of a key for accessing the value information itself and value informationand value information to a value information service device which holds the logic safely from an information recording medium of a moved material.
A means to relay download of value information from said value information service device to an information recording medium of a movement destination.

[Claim 12]A means to change a key for accessing value information on an information recording medium of a moved material into **** from this key at the time of normal use before relaying upload to a value information service deviceThe value information move service device according to claim 11 having further a means to change into this key from **** after downloading value information from a value information service device on an information recording medium to a movement destination.
[Claim 13]When there are two or more keys for two or more value information being held on an information recording medium of a moved materialand accessing each value information itself and value information and value information service devices which hold the logic safelyThe value information move service device according to claim 11 characterized by what a means to relay a means to relay said uploadand/or said download relays for every value information service device.
[Claim 14]The value information move service device according to claim 11 characterized by what it has further a means to perform initialization processing of an information recording medium of a movement destination for.
[Claim 15]The value information move service device according to claim 11 characterized by what it has further for a means which carries out authenticating

processing of an information recording medium of a moved materialand/or the information recording medium of a movement destination.
[Claim 16]A value information move service method which serves movement of value information between information recording mediacomprising:
A step which relays upload of a key for accessing the value information itself and value informationand value information to a value information service device which holds the logic safely from an information recording medium of a moved material.
A step which relays download of value information from said value information service device to an information recording medium of a movement destination.

[Claim 17]A step which changes a key for accessing value information on an information recording medium of a moved material into **** from this key at the time of normal use before relaying upload to a value information service deviceThe value information move service method according to claim 16 having further a step changed into this key from **** after downloading value information from a value information service device on an information recording medium to a movement destination.
[Claim 18]When there are two or more keys for two or more value information being held on an information recording medium of a moved materialand accessing each value information itself and value information and value information service devices which hold the logic safelyThe value information move service method according to claim 16 characterized by what a step which relays a step which relays said uploadand/or said download is performed for for every value information service device.
[Claim 19]The value information move service method according to claim 16 characterized by what it has further for a step which performs initialization processing of an information recording medium of a movement destination before downloading value information from a value information service device.
[Claim 20]The value information move service method according to claim 16 characterized by what it has further for a step which carries out authenticating processing of an information recording medium of a moved materialand/or the information recording medium of a movement destination.
[Claim 21]A storage which stored physically computer software described to perform value information move service which serves movement of value information between information recording media on computer systems in computer-readable formcomprising:
A step which relays upload of a key for said computer software to access an information recording medium to the value information itself and value information of a moved materialand value information to a value information service device which holds the logic safely.
A step which relays download of value information from said value information service device to an information recording medium of a movement destination.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the non-contact (or contact type) IC card or IC chip to a memory which can be written according to non-contact while being provided with the memory function holding dataWhile having a wireless interface for wireless data to perform access to a memory function from external reader/writer especiallyIt is related with information processing terminalssuch as a noncontact IC card or an IC chip provided with the cable interface for connecting with an external instrument and a portable telephone used by carrying this kind of an IC card or an IC chip via a cable interfaceand PDA.
[0002]The noncontact IC card or IC chip in which this invention stored electronically the value information of electronic moneyan electronic ticketand others in detailAnd the information processing terminal used by carrying this kind of an IC card or an IC chip via a cable interface is startedand it is especially related with secure movement of the value information between information processing terminals.
[0003]
[Description of the Prior Art]From the formervarious devices which used the password and the password for personal identification or authenticating processing are devisedand practical use is presented. For examplein a bank or other financial institutionswhen using an ATM card and a credit card. the banking terminal top of a cash dispenser or others -- the person himself/herself -- the input of a password or a password is demanded from a user as a means of attestationand after checking that the right password and the password have been entered from the usercash-receipt-and-disbursement operation is performed.
[0004]In storagessuch as a magnetic stripe currently allocated on one ATM cardonly the usable storage area is provided only to the bank. Thereforesince the input of a password or a password which was mentioned above is only access to this single storage areait is hard to say that the protection to forgery or surreptitious use is enough.
[0005]For this reasonthe contact type IC card which had an electric point of contact in an ATM carda credit cardetc.and the noncontact IC card which write data by non-contact via wireless data are often increasingly used from viewpoints of forgery prevention etc. For examplethe IC card reader/writer installed in the entrance in a cash dispenser or the concert hallthe wicket of a stationetc. can access the IC card which the user held up by non-contact.
[0006]Personal identification or authenticating processing is performed between an IC

cardand an IC card reader/writer by a user inputting a password into the IC card reader sideand comparing the inputted password with the password stored on the IC card. And when it succeeds in personal identification or authenticating processinguse of the application saved in the IC card is attainedfor example. Hereas application which an IC card holdsthe value information of electronic moneyan electronic ticketetc. can be mentionedfor example. It is also possible by storing an advance payment system certificate electronically to use the personal digital assistant connected to an IC card or this as a prepaid card. (The password used at the time of IC card access is called especially PIN (PersonalIdentification Number).)

[0007]These daysan IC card with conjointly comparatively mass memory space appearsand improvement in minuteness making art is spreading. Since a single storage areai.e.single applicationis supported in the conventional ATM card etc.it is necessary to walk around with two or more cards which responded for every use or purpose. On the other handsince two or more applications are simultaneously storable according to such an IC card with a bulk memorythe IC card of one sheet can be used for two or more uses. For exampletwo or more applicationssuch as electronic money for performing electronic bankingan electronic ticket for entering the specific concert halland a digitized advance payment system certificateare stored on the IC card of one sheetand the IC card of one sheet can be made to apply to various uses.

[0008]By having a cable interface for an IC card to connect with an external instrument other than the non-contact (or contact type) interface to the reader/writer for cards (card reading-and-writing device)It can connect with a portable telephone and PDA (Personal Digital Assistant)or an IC card can be built in and used (howeverin the case of many which are built in a terminalan IC card is one-chip-ized and is constituted).

[0009]In such a casevarious application services using an IC card can be performed on an information processing terminal. For examplethe user interaction to an IC card can be performed on an information processing terminal using user interfacessuch as a keyboard on an information processing terminaland a display. By connecting the IC card with the portable telephonea telephone network is passed and the contents memorized on the IC card can also be carried out.

[0010]Of coursewhen value informationsuch as electronic moneyan electronic ticketan advance payment system certificateis stored on an IC cardthe information processing terminal can realize processing of value informationsuch as electronic banking and settlement of a prepaid card formand other various services. The processing according to the phase of the data transfer between an IC card and a card reading-and-writing device and the processing according to the internal state of the IC card can be provided.

[0011]By the waywhen the IC chip which stored value information is built in a portable telephoneit is necessary to move value information between IC chips (i.e.between personal digital assistants) for the reasons of a model change etc.

[0012]Generally model change procedure of a portable telephone is performed at the store of a telecommunications companyetc.and the personal information on the address book within an old machine kindetc. is moved to a new model. Howeverwhen moving the value information in an IC chipthe illegal duplicate and alteration of disappearance of value information and value information by communication failurea machine obstacleetc. in the middle of a move may be performedand responsibility is excessive for a telecommunications company.
[0013]First of allsince a telecommunications company has neither a key required in order to access the value information instead of one with the service provider of electronic money or an electronic ticketnor its logicprocessing value information has much inconvenience. In a telecommunications companythe responsibility about value information and its key occurs inevitably by contracting movement of value information. For the service provider of electronic money or an electronic ticketit is not preferred to pass the access key used as the basis of trust of service and its logic outsidealthough it is a telecommunications company.
[0014]The service provider of value information has usually shut up the key for accessing the value information itself and value informationand its logic using hardware module SAM (Secure Application Module) with the Tampa-proof nature. in order to move two or more value information by one servers for movementsuch as a telecommunications companybe temporaryalthough it is necessary to save value informationUnless a thing like SAM is usedeven if it enciphers uniquely by this server for movementa possibility of decoding value information and its key on a server becomes high.
[0015]On the other handapart from the model change procedure of the main part of a personal digital assistantthe method of moving the value information in an IC chip by the service provider of the value information is also considered. Probablythis method will be effective from a viewpoint of responsibility separation.
[0016]Howeverthe user has to take two or more procedure in connection with the model change of a personal digital assistant. When the value information of various sorts is especially stored in one IC chip with increase of the memory space of an IC card or an IC chipthe move procedure of value information must be taken to each service providerand it is very troublesome. Although the reader/writer which reads value information from an IC chip needs to switch a session to two or more service providersit requires time and effort for performing this switching operation manually. Since the structure of communication by the side of an IC chip also becomes complicateda possibility that an obstacle will occur becomes high.
[0017]
[Problem(s) to be Solved by the Invention]The purpose of this invention is to provide the outstanding data transfer system and data transfer method and value information move service device which can be made to move the value information of electronic moneyan electronic ticketetc. to secure onea value information move service

methodand a storage.
[0018]. The further purpose of this invention can move the value information of the electronic money currently held in the IC card or the IC chipan electronic ticketetc. to secure one. It is in providing the outstanding data transfer system and a data transfer methoda value information move service devicea value information move service methodand a storage.
[0019]The further purpose of this invention two or more value information currently held in the IC card or the IC chipIt is in providing the outstanding data transfer system and data transfer method and value information move service device which can be moved to secure one only by connecting with one servera value information move service methodand a storage.
[0020]
[Means for Solving the Problem and its Function]This invention is made in consideration of an aforementioned problemand the 1st sideA key for accessing the value information itself and value information which are the data transfer systems for moving value informationand serve as a moved objectand a value information service device which holds the logic safelyA value information move service device which relays upload to said value information service device of value information stored in an information recording medium of a moved materialand download of value information from said value information service device to an information recording medium of a movement destinationIt is a providing data transfer system.
[0021]Howevera "system" said here means a thing in which two or more devices (or functional module which realizes a specific function) gathered logicallyand it is not especially asked whether each device and a functional module are in a single case.
[0022]The 2nd side of this invention is a data transfer method for moving value informationA step which relays upload of a key for accessing the value information itself and value informationand value information to a value information service device which holds the logic safely from an information recording medium of a moved materialIt is a data transfer method possessing a step which stores temporarily value information which a value information service device is movingand a step which relays download of value information from said value information service device to an information recording medium of a movement destination.
[0023]According to a data transfer system or a data transfer method concerning the 1st or 2nd side of this invention. . Shut up a key required in order to access value information currently held at information recording mediasuch as an IC chipat value information of the value information itselfand its logic. Value information service devicessuch as hardware module SAM with the Tampa-proof natureare controlledIt can move secure one on other information recording mediapreventing a duplicate and an alteration of value informationwithout showing the logic as a key required in order to access the value information itself and value information in addition to a device with authority. For examplewhen exchanging a personal digital assistant for a new

modelall the value information currently held in a terminal only by connecting with one place can be moved to secure one. Thereforethe responsibility range of a move entrepreneur of value information and each service provider who employs value information service is clearly separable.

[0024]Said value information move service device may be made to upload value information to said value information service device hereafter changing a key for accessing value information on an information recording medium of a moved material into **** from this key at the time of normal use. In such a casevalue information can prevent a duplicate and being altered and used unjustly in the middle of movement. Even if it is a case where movement of value information goes wrongby returning a key of a moved material to this keyit can use as backup and disappearance of value information can be prevented.

[0025]After said value information move service device downloads value information from said value information service device on an information recording medium to a movement destinationit may be made to change it into this key from ****. In such a casesince it becomes impossible with as about normal use by considering value information left behind to an information recording medium of a moved material as as [****]an unauthorized use can be prevented.

[0026]When there are two or more keys for two or more value information being held on an information recording medium of a moved materialand accessing each value information itself and value information and value information service devices which hold the logic safelySaid value information move service device may be made to perform upload of value information from an information recording medium of a moved materialand download to an information recording medium of a movement destination for every value information service device. In such a casewhat is necessary is just to connect with one value information move service deviceand it is not necessary to switch communication one by one for every value information service hand control or automatically. For this reasontime and effort can decrease and a possibility that communication failure will be encountered can be decreased. If it thinks from the information-recording-medium side of a moved materialhe does not need to be conscious of each value information service device used as a relay destinationand procedure will be simplified.

[0027]Said value information move service device may be made to perform initialization processing of an information recording medium of a movement destinationbefore downloading value information from a value information service device.

[0028]Said value information move service device may be made to carry out authenticating processing of an information recording medium of a moved materialand/or the information recording medium of a movement destination.

[0029]The 3rd side of this invention is a value information move service device or a value information move service method which serves movement of value information

between information recording mediaA means or a step which relays upload of a key for accessing the value information itself and value informationand value information to a value information service device which holds the logic safely from an information recording medium of a moved materialIt is a value information move service device or a value information move service method possessing a means or a step which relays download of value information from said value information service device to an information recording medium of a movement destination.

[0030]According to a value information move service device or a value information move service method concerning the 3rd side of this invention. . Shut up a key required in order to access value information currently held at information recording mediasuch as an IC chipat value information of the value information itselfand its logic. Value information service devicessuch as hardware module SAM with the Tampa-proof natureare controlledIt can move secure one on other information recording mediapreventing a duplicate and an alteration of value informationwithout showing the logic as a key required in order to access the value information itself and value information in addition to a device with authority. For examplewhen exchanging a personal digital assistant for a new modelall the value information currently held in a terminal only by connecting with one place can be moved to secure one. Thereforethe entrepreneur who performs a model change of a personal digital assistant can move value informationseparating clearly the responsibility range of each service provider who employs value information service.

[0031]A value information move service device concerning the 3rd side of this invention may be made to upload value information to said value information service device hereafter changing a key for accessing value information on an information recording medium of a moved material into **** from this key at the time of normal use. In such a casevalue information can prevent a duplicate and being altered and used unjustly in the middle of movement. Even if it is a case where movement of value information goes wrongby returning a key of a moved material to this keyit can use as backup and disappearance of value information can be prevented.

[0032]After downloading value information from said value information service device on an information recording medium to a movement destinationit may be made to change into this key from ****. In such a casesince it becomes impossible with as about normal use by considering value information left behind to an information recording medium of a moved material as as [****]an unauthorized use can be prevented.

[0033]When there are two or more keys for two or more value information being held on an information recording medium of a moved materialand accessing each value information itself and value information and value information service devices which hold the logic safelyIt may be made to perform upload of value information from an information recording medium of a moved materialand download to an information recording medium of a movement destination for every value information service

device. In such a casewhat is necessary is just to connect with one value information move service deviceand it is not necessary to switch communication one by one for every value information service hand control or automatically. For this reasontime and effort can decrease and a possibility that communication failure will be encountered can be decreased. If it thinks from the information-recording-medium side of a moved materialhe does not need to be conscious of each value information service device used as a relay destinationand procedure will be simplified.

[0034]A value information move service device or a value information move service method concerning the 3rd side of this invention may be made to perform initialization processing of an information recording medium of a movement destinationbefore downloading value information from a value information service device.

[0035]A value information move service device or a value information move service method concerning the 3rd side of this invention may be made to carry out authenticating processing of an information recording medium of a moved materialand/or the information recording medium of a movement destination.

[0036]The 4th side of this invention is the storage which stored physically computer software described to perform value information move service which serves movement of value information between information recording media on computer systems in computer-readable formA step which relays upload of a key for said computer software to access an information recording medium to the value information itself and value information of a moved materialand value information to a value information service device which holds the logic safelyIt is a storage possessing a step which relays download of value information from said value information service device to an information recording medium of a movement destination.

[0037]A storage concerning the 4th side of this invention is a medium which provides computer software in a computer-readable form to a general purpose computer system which can execute various program codesfor example.Attachment and detachment of DVD (Digital Versatile Disc)CD (Compact Disc)FD (Floppy Disk)MO (Magneto-Optical disc)etc. are free for such a mediumand it is a storage of portabilityfor example. Or it is also technically possible to provide specific computer systems with computer software via transmission mediasuch as a network (a network does not ask distinction of radio and a cable)etc.

[0038]A storage concerning the 4th side of this invention defines a collaboration relation on structure of computer software and a storage for realizing a function of predetermined computer softwareor a function on computer systems. By installing predetermined computer software in computer systems via a storage concerning the 4th side of this inventionif it puts in another wayOn computer systemsa collaboration operation is demonstrated and the same operation effect as a value information move service device or a value information move service method concerning the 3rd side of this invention can be obtained.

[0039]The purposethe featureand an advantage of further others of this invention will

become clear [rather than] by detailed explanation based on an embodiment and a drawing to attach of this invention mentioned later.
[0040]
[Embodiment of the Invention]Hereafterit explains in detail about the embodiment of this inventionreferring to drawings.
[0041]This invention moves to secure one two or more value information currently held in the IC card or the IC chip only by connecting with one server. Belowthe thing of the server which moves value information is made to call it a "value move server." For examplewhen moving the value information on the IC chip built in on the occasion of the model change of a portable telephonethe telecommunications company etc. which offer model change service should just manage a value move server. With the provider of each value information servicealthough not necessarily unifiedsince the value move server can move value information to secure one according to this inventionseparation of responsibility becomes clear and it does not become excessive [the responsibility of the entrepreneur who manages a value move server].
[0042]The composition of the network system which realizes secure movement of value information is typically shown in drawing 1.
[0043]As shown in the figureon networkssuch as VPN (Virtual Private Network) or a dedicated lineThe application server (APS) 10A which the provider who offers value information service of electronic moneyan electronic ticketetc. installs10B--and the value move server 20 for moving the value information built in the IC card or the IC chip to secure one between IC chips exist.
[0044]Each application server (APS) 10A10B--and the server 20 for value movement are provided with hardware module SAM (Secure Application Module) which has the Tampa-proof naturerespectively. SAM has shut up the key for accessing the value information itself and value informationand its logic.
[0045]According to this embodimentthe server 20 for value movement is provided with administrative SAM21 in order to manage the information in each IC chip to secure one. Administrative SAM21 manages each IC chip holding value informationsuch as initialization processing of an IC chip. When administrative SAM21 moves the value information in an IC chipit is provided with the logic for changing into temporary "****" which uses it from "this key" at the time of normal use only at the time of movement.
[0046]Each application server 10A-- is provided with SAM12 for movement which operates at the time of movement by **** which operates with this key used when carrying out normal use of the value informationand which SAM11 and administrative SAM21 of the server 20 for value movement usually publish.
[0047]UsuallySAM11 is individually managed on each service provider application server 10and serves value information. Usuallyeach service provider who gets to know the key with which SAM11 accesses value informationand its logic cannot usually know the inside of SAM11unless each others have authority. The server 20 for value

movement cannot usually know the contents of SAM11either.
[0048]UsuallyphysicallySAM11 and SAM12 for movement may be the hardware modules which became independent separatelyeven if unified within the same hardware module. The service provider may arrange SAM by a contract etc. at somewhere elsesuch as not the application server that self manages but the server 20 for value movement.
[0049]Although it is also possible to constitute as a server apparatus by hardware for exclusive useeach application server 10 and the server 20 for value movementIt is realizable also with the gestalt of starting predetermined server application on the common computer system called a workstation (WS) and a personal computer (PC). An example of a computer system is the PC / AT compatible machine or its succeeding machine of U.S. IBM.
[0050]The IC card is built in and used for the personal digital assistants 30Asuch as a portable telephone and PDA (Personal Digital Assistant)as an IC chipor non-contact (or contact) access is carried outand it is used for the personal digital assistant 30B with reader/writer. In moving value information between an IC chip or an IC card for exchange of the model change of a personal digital assistantor the IC card itselfit connects with VPN via the communication media of radio or a cableand the personal digital assistant 30 requests movement of value information from the value move server 20. According to this embodimenteven if you are a case where two or more value information held at the IC chip is movedthe personal digital assistant 30 should care about enough the point that what is necessary is just to connect with the one value move server 20.
[0051]When moving value informationthe server 20 for value movement uses administrative SAM21and controls an IC chip via a channel.
[0052]According to this embodimentthe server 20 for value movement bears the role which relays itwhen encryption communication is performed between SAM12 for movement of each service providerand an IC chip using administrative SAM21 for movement of value information. The personal digital assistant 30B and the IC chip built-in personal digital assistant 30A with the reader/writer function by the side of an IC chip bear the role which makes connection between an IC chip and the value move server 20when encryption communication is performed between SAM and an IC chip.
[0053]Between the server 20 for value movementand each SAM12 for movementsetting out is individually made possiblerespectively about the authority to control SAM12 for movement with the server 20 for value movement. Encryption by PKI (Public Key Infrastructure: public key infrastructure) or a common key is possible for between the server 20 for value movementand each SAM12 for movement. Between the server 20 for value movementand remote SAM12 for movementit is connected by VPN or a dedicated line.
[0054]In the network system shown in drawing 1in order to move the value

information in the IC chip built in the IC card or the personal digital assistantthe connection destination of the IC chip used as a moved material and a movement destination serves as the single server 20 for value movement.
[0055]Administrative SAM21 of the server 20 for value movement changes the key of value information into temporary "****" for movement from "this key" at the time of normal usebefore moving value information. Before no movement of the value information currently held in the IC chip is completedposition information on the original IC chip is not deleted yetbut it holds as an object for backup.
[0056]When movement is completedthe normal use of value information of administrative SAM21 becomes possible by returning **** to this key in the IC chip of a movement destination. Since it becomes impossible with as about normal use by considering it as as [****] about the IC chip side of the move origin which it left to backupan unauthorized use can be prevented.
[0057]The server 20 for value movement moves using SAM12 for movement of the service provider who corresponds each value information in an IC chip. Under the present circumstancesin SAM12 for movement by the side of a service provider (APS)the access restriction from the server 20 for value movement is set up a priori.
[0058]In a service provider's application server 10 sidewhile usually storing the key and logic for accessing value information at the time of normal use in SAM11the key for value information movement and its logic are stored in SAM12 for movement. The value information in an IC chip is temporarily saved in SAM12 for movement of the application server 10 at the time of movement.
[0059]At the IC chip side used as the movement destination of value informationafter performing pretreatment predetermined [such as formatting of the memory area]by the server 20 course for value movement. The movement is completed by downloading value information from SAM12 for movement of the service provider 10i.e.an application server.
[0060]After movement makes it impossible to move value information with the same key for movement henceforthwhen administrative SAM21 changes into a right key. It becomes impossible as a resultto use the value information for backup which remains on the IC chip of a moved material.
[0061]And completion of movement of all the value information in an IC chip will delete the value information temporarily saved in SAM12 for movement of a service provider.
[0062]In the form of the flow chart shows the procedure for moving value information to secure one between IC chips to drawing 2 on the network system concerning this embodiment. This procedure is realized by the collaboration operation between the IC chip by which network connection is carried out via a personal digital assistantthe server 20 for value movementand SAM12 for movement of each applicable application server (provider) 10. Hereafterthe secure moving processing of value information is explainedreferring to this flow chart.

[0063]Firstthe IC chip which becomes the move origin of value information is connected with the communication apparatus (for examplea portable telephone with reader/writer or a portable telephone with a built-in IC chip) 30 with a reader/writer function. The IC chip of a moved material is connected with the server 20 for value movement by this communication apparatus 30 courseand it attests with the server 20 for value movement with the user ID and the password which are sent from the communication apparatus 30 (Step S1).
[0064]The server 20 for value movement searches the inside of the moved material IC chip of value informationand it saves those information in the movement information database (not shown) of server 20 local while it detects the kind of all the value information registered into the IC chip. Or the serial number and the registered reference table of the kind of value information of the IC chip which the server 20 side for value movement prepared a priori are prepared in the movement information database a prioriBy obtaining the serial number of the moved material IC chip of value informationthe kind of value information registered into the IC chip is traced using this reference table (Step S2). The application servers which preparecorresponding service provideri.e.SAMshall differ for every kind of value information.
[0065]Subsequentlyadministrative SAM21 of the server 20 for value movement changes a key required in order to access the value information in the moved material IC chip of value information itself into "****" temporarily used from "this key" at the time of normal use at the time of movement (Step S3). As a resulton a moved material IC chipit will be in the state which cannot use the usual value information during movement of value information. That isaccess to the value information in an IC chip is attained by switching to **** by SAM12 for movement instead of [it becomes impossible for usual SAM11 of an applicable service provider to access the value information in an IC chip].
[0066]Subsequentlythe server 20 for value movement takes out one service provider searched out of the IC chip (step S4). And administrative SAM21 of the server 20 for value movement starts movement of value information per kind (application units) of value information.
[0067]FirstSAM12 for movement of the service provider 10i.e.an application serverwhich manages the value information to which it is made to move first is specifiedand the IC chip of the move origin of value information is made to communicate with the SAM12 for movement (Step S5).
[0068]The IC chip of value move origin performs SAM12 for movementand mutual recognition with the key in a chip about a certain value information in the chip concernedand begins encryption communication (Step S6).
[0069]Subsequentlythe value information in the moved material IC chip of value information is copied to the memory area in SAM12 for movement by the side of the application server 10 (Step S7). (namelyupload of value information)
[0070]After the copy to the memory area in SAM12 for movement of value

information is completedSAM12 for movement of the service provider who manages the following moved object value information is specifiedand a moved material IC chip is made to communicate with the SAM12 for movement by the same procedure as ****. Thenstep S4S5S6and S7 are repeated until it finishesthe copyi.e.uploadof all the value information in a moved material IC chip(Step S8).

[0071]In other wordsthe number of the servers 20 for value movement which the moved material IC chip of value information connects is oneandso to speakthis server 20 for value movement relays communication with the IC chip of a moved materialand each SAM12 for movement of a service provider.

[0072]After the copy of each service provider's SAM12 for movement completes all the value information in a moved material IC chip (i.e.after upload of value information is completed)shortlyThe communication apparatus (for examplea portable telephone with a reader/writer function and the portable telephone having an IC chip) 30 with the reader/writer function in which the movement destination IC chip of value information was connectedIt connects with the server 20 for value movementand attests with the server 20 for value movement with the user ID and the password which are sent from a communication apparatus (step S9).

[0073]By certification information with the movement destination IC chip of value informationadministrative SAM21 of the server 20 for value movement searches a movement information databaseand acquires the initialization (format) information on this movement destination IC chip. And administrative SAM21 of the server 10 for value movement initializes the memory area of a movement destination IC chip based on this initialization information (Step S10). On the occasion of this initializationnot this key used at the time of use of value information but **** for value information movement is used.

[0074]Subsequentlythe server 20 for value movement takes out one service provider from a movement information database (Step S11). And the server 20 for value movement starts movement of value informationi.e.the download to an IC chipper kind (application units) of value information.

[0075]FirstSAM12 for movement of a service provideri.e.an application serverwhich manages the value information to which it is made to move first is specifiedand the IC chip of the movement destination of value information is made to communicate with the SAM12 for movement (Step S12).

[0076]And the IC chip of the movement destination of value information uses it about a certain value informationthe keyi.e.****in the chip set at the time of initializationperforms SAM12 for movementand mutual recognitionand begins encryption communication (Step S13).

[0077]Subsequentlythe value information copied namelyuploaded out of the moved material IC chip of value information to the memory area in SAM12 for movement is copied namelydownloaded in the movement destination IC chip of value information (Step S14).

[0078]After a copy into the movement destination IC chip about a certain value information is completedSAM12 for movement of the service provider who manages the value information which serves as a moved object next is specifiedand a movement destination IC chip is made to communicate with the SAM12 for movement by the same procedure as ****. ThenStep S11S12S13and S14 are repeated until the copy of all the value information into a movement destination IC chip finishes (Step S15).
[0079]In other wordsthe number of the servers 20 for value movement which the movement destination IC chip of value information connects is oneandso to speakthis server 20 for value movement relays communication with the IC chip of a movement destinationand SAM12 for movement of each service provider.
[0080]If movement of all the value information is completedthe server 20 for value movement will change **** for value information movement of a value movement destination IC chip into this key at the time of normal use (Step S16). As a resultin the IC chip side of a movement destinationthe normal use of value information becomes possible. Since it becomes impossible with as about normal use by considering it as as [****] about the IC chip which it left to backupan unauthorized use can be prevented. The value information left behind in the IC chip of a moved material is deleted if needed.
[0081]The server 20 for value movement clears the value information for movement saved at the memory area in SAM21 for movement of each application server 10 related to movement of value information (Step S17).
[0082]The processing procedure for uploading the value information currently held at the moved material IC chip to SAM12 for movement of each service provider is shown in drawing 3. Hereafterthe collaboration operation between each person for uploading value information from a moved material IC chip to SAM12 for movement is explainedreferring to the figure.
[0083]Firstthe IC chip which becomes the move origin of value information is connected with the communication apparatus (for examplea portable telephone with reader/writer or a portable telephone with a built-in IC chip) 30 with a reader/writer functionand a communication apparatus acquires the serial number of an IC chipetc.
[0084]Subsequentlyafter the communication apparatus with a reader/writer function performing user authentication between the servers 20 for value movement and succeeding in attestationreservation of the channel for IC chip control is required of this communication apparatusand a channel is secured.
[0085]Subsequentlyso that a key required in order that the server 20 for value movement may access the value information in a moved material IC chip itself to administrative SAM21 may be changed into "****" temporarily used from "this key" at the time of normal use at the time of movementRequesting key changeadministrative SAM21 performs this key change processing. By having been changed into **** from this keynot SAM11 but SAM12 for movement can usually

access now the value information of a moved material IC chip by the applicable service provider 10 side.
[0086]Subsequentlythe server 20 for value movement requests move (upload) processing of value information to the service provider 10 who manages value information.
[0087]In the service provider 10 sidea request of this value information moving processing is answeredand SAM12 for movement publishes the upload request of value information to a moved material IC chip. On the other handa moved material IC chip performs a copyi.e.uploadfor value information to SAM12 for movement.
[0088]Only a required service provider's part carries out repeat execution of a value information moving processing requesta value information upload requestand the upload of value information.
[0089]The processing procedure for downloading the value information uploaded to SAM12 for movement of the service provider to the IC chip of a movement destination is shown in drawing 4. Hereafterthe collaboration operation between each person for downloading value information from SAM12 for movement to a movement destination IC chip is explainedreferring to the figure.
[0090]Firstthe IC chip which becomes the move origin of value information is connected with the communication apparatus (for examplea portable telephone with reader/writer or a portable telephone with a built-in IC chip) 30 with a reader/writer functionand a communication apparatus acquires the serial number of an IC chipetc.
[0091]Subsequentlyafter the communication apparatus with a reader/writer function performing user authentication between the servers 20 for value movement and succeeding in attestationreservation of the channel for IC chip control is required of this communication apparatusand a channel is secured.
[0092]If a channel is securedadministrative SAM21 of the server 20 for value movement will search a movement information database by the serial number of a movement destination IC chipand will acquire the initialization (format) information on this movement destination IC chip. And administrative SAM21 of the server 10 for value movement initializes the memory area of a movement destination IC chip based on this initialization information. This is notified to administrative SAM21 that initialization ends a movement destination IC chip.
[0093]Subsequentlythe server 20 for value movement requests move (download) processing of value information to the service provider 10 who manages value information.
[0094]In the service provider 10 sidea request of this value information moving processing is answeredand SAM12 for movement downloads the value information uploaded to the own memory area to the IC chip of a movement destination. On the other handthis is notified that download completes the IC chip of a movement destination.
[0095]A value information moving processing requesta value information download

requestand the download terminating notice of value information carry out repeat execution only of a required service provider's part.
[0096]And when download of all the value information is completedthe server 20 for value movementKey change is requested and administrative SAM21 performs this key change processing so that a key required in order to access the value information in a movement destination IC chip itself to administrative SAM21 may be changed into "this key" temporarily used from "****" at the time of normal use at the time of movement. By having been returned to this key from ****not SAM12 for movement but usual SAM11 can access now the value information of a moved material IC chip by the applicable service provider 10 side.
[0097]As a resultin the IC chip of a movement destinationthe normal use (for exampleelectronic banking by electronic moneyuse of an electronic ticketetc.) of value information becomes possible. Since it becomes impossible with as about normal use by on the other hand considering it as as [****] about the IC chip side of the move origin which it left to backupan unauthorized use can be prevented. The value information left behind in the IC chip of a moved material is deleted if needed.
[0098]In drawing 5 and drawing 5the structure of the non-contact data communications between an IC cardand a card reader/writer is illustrated.
[0099]Radio between reader/writer and an IC card is realizedfor example based on the principle of electromagnetic induction. In drawing 5the structure of the radio of the reader/writer and the IC card based on electromagnetic induction is illustrated notionally. Reader/writer is provided with antenna L_{RW} which comprised a loop coiland a magnetic field is generated by passing current I_{RW} to this antenna L_{RW} around it. On the other handloop coil L_c is electrically made with the IC card side around the IC card. At the loop coil L_c end by the side of an IC cardthe induced voltage by the magnetic field which loop antenna L_c by the side of reader/writer emits arisesand it is inputted into the terminal of an IC card connected to the loop coil L_c end.
[0100]Although the degree of coupling changes according to mutual physical relationshipantenna L_{RW} by the side of reader/writer and loop coil L_c by the side of an IC card can be realized to form one transformer as a systemand as shown in drawing 6they can be modeled.
[0101]At the reader/writer sidein modulating current I_{RW} passed to antenna L_{RW}voltage V_O induced by loop coil L_c on an IC chip can receive abnormal conditionsand the reader/writer can perform data transmission to an IC card using that.
[0102]An IC card has the function (Load Switching) to fluctuate the load between the terminals of loop coil L_c according to the data for returning reader/writer. If the load between the terminals of loop coil L_c is changedin the reader/writer sidethe impedance between antenna terminals changesand it will become change of passing current I_{RW} of antenna L_{RW}or voltage $V_{RW}$and will appear. By restoring to a part for this changethe reader/writer can receive the returned data of an IC card.
[0103]Namelythe IC card can communicate by applying amplitude modulation to the

signal which appears in the receiving circuit by the side of reader/writer by changing the load between own antennas according to the reply signal over the question signal from reader/writer.

[0104]The internal hardware constitutions of the personal digital assistant 110 of the type having IC chip 100 are typically shown in drawing 7. It is equivalent to the personal digital assistant 110 said here at information processing terminalssuch as a portable telephone and PDA (Personal Digital Assistant). If it is a portable telephoneit will be connected to VPN or a dedicated line via a radio telephone network. If it is a personal digital assistantit will be connected to VPN or a dedicated line via a radio telephone network via other portable telephones.

[0105]As shown in the figureIC chip 100 comprises the antenna section 101the analog part 102the digital-control part 103the memory 104and the external interface 105.

[0106]The antenna section 101 transmits and receives non-contact data between the reader/writers 200. The analog part 102 processes the analog signal transmitted and received from the antenna sections 101such as detectiona strange recoveryand clock extraction. IC chip 100 can communicate by applying amplitude modulation to the signal which appears in the receiving circuit by the side of reader/writer by changing the load between own antennas according to the reply signal over the question signal from the reader/writer 200.

[0107]The digital-control part 103 controls processing of transmitted and received data and the operation in other IC cards in generalization. The digital-control part 103 has connected locally the memory 104 in which an address is possibleSince store applicationssuch as electronic money and an electronic ticketthe program code which the digital-control part 103 executes is loaded or the work data under execution is savedit can be used.

[0108]Various applications are stored in the memory 104 of IC chip 100. As applicationthe value information of electronic moneyan electronic ticketetc. can be mentionedfor example.

[0109]The non-contact interface with which the external interface 105 connects the reader/writer 200 is a functional module for the digital-control part 103 to connect with personal digital assistant 110 main part with a different interface protocol. The data written in the memory 104 can be transmitted to the personal digital assistant 110 main-part side via the external interface 105.

[0110]According to this embodimenta cable interface like UART or I^2C is used for the external interface 105 which connects built-in IC chip 100 with the personal digital assistant 110. Howeverthe interface specification in particular of the external interface 105 may not be limitedmay be other cable interfacesor may be wireless interfacessuch as Bluetooth and IEEE.802.11b.

[0111]IC chip 100 can be driven by the reception radio wave from the card reading-and-writing device received by antenna section 101 coursefor example. Of courseit may be constituted so that all may operate in part with the power supply from the

personal digital assistant 110 side.
[0112]On the other handthe personal digital assistant 110 main-part side comprises the program control part 111the indicator 112and the user input part 113.
[0113]The program control part 111 uses RAM for workspacefor example according to a microprocessorRAMand the program code with which it comprised a ROM (neither is illustrated) and the microprocessor was stored in ROMand various processing services are performed. The processing to IC chip 100 is included in processing service besides original functions of personal digital assistant 110such as a portable telephone and PDA.
[0114]The program control part 111 is external-interface 105 courseand can access IC card 100.
[0115]The information storing part 114 is formed in the program control part 111. The information storing part 114 comprises a storage device in which writing like EEPROM (Electrically Erasable and Programmable ROM) is possibleexternal storagessuch as a hard disketc.for example.
[0116]The indicator 112 comprises a liquid crystal display (LCD:liquid Crystal Display)for example. The indicator 112 can carry out the picture output of the processing result in the program control part 111etc.and can notify a user of themfor example.
[0117]The user input part 113 comprises a keyboarda jog dialor a touch panel on which the display screen of the indicator 112 was overlappedand in order that a user may input a command and data into the personal digital assistant 110it is used.
[0118]The program control part 111 in the personal digital assistant 110 is driven by electric supply from the main power supply which is not illustrated [battery].
[0119]By holding up the personal digital assistant 110 having IC chip 100 to the reader/writer (R/W) 200non-contact data communications are started between built-in IC chip 100 and the reader/writer 200. And access to the value information of the electronic ticket in IC chip 100electronic moneyetc. is permitted through collation of passwordssuch as PIN.
[0120][Supplement] It has explained in detail about this inventionreferring to a specific embodiment above. Howeverit is obvious that a person skilled in the art can accomplish correction and substitution of this embodiment in the range which does not deviate from the gist of this invention. That isthis invention should not be indicated with the gestalt of illustrationand the description content of this specification should not be interpreted restrictively. In order to judge the gist of this inventionthe column of the claim indicated at the beginning should be taken into consideration.
[0121]
[Effect of the Invention]As a full account was given aboveaccording to this inventionthe outstanding data transfer system and data transfer method and value information move service device which can be made to move the value information of

electronic moneyan electronic ticketetc. to secure onea value information move service methodand a storage can be provided.
[0122]. According to this inventionthe value information of the electronic money currently held in the IC card or the IC chipan electronic ticketetc. can be moved to secure one. The outstanding data transfer system and a data transfer methoda value information move service devicea value information move service methodand a storage can be provided.
[0123]Two or more value information which is held in the IC card or the IC chip according to this inventionThe outstanding data transfer system and data transfer method and value information move service device which can be moved to secure onea value information move service methodand a storage can be provided only by connecting with one server.
[0124]It is not necessary to save the access key and the value information itself of value information for movement at the server for value movementandaccording to this inventionit is saved in SAM of the service provider who employs value information. Thereforethe responsibility range of the move entrepreneur of value information and each service provider who employs value information service is clearly separable.
[0125]According to this inventionwhen two or more value information in an IC chip must be movedit is enough as each communication apparatus for the moved material IC chip of value informationand the movement destination IC chip of value information just to connect only with one server for value movement. Thereforethe communication apparatus does not need to switch communication one by one for every value information service hand control or automatically. For this reasontime and effort can decrease and a possibility that communication failure will be encountered can be decreased. In this caseif it thinks from the IC chip side and will be connected with one server for value movementhe does not need to be conscious of existence of SAM of each service provider who becomes a relay destination.
[0126]According to this inventionsince the key for accessing to value information before movement is changed into "****" and he is trying to return to this key after the completion of a movevalue information can prevent a duplicate and being altered and used unjustly in the middle of movement. Even if it is a case where movement of value information goes wrongdisappearance of value information can be prevented by returning the key of a moved material to this key.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing typically the composition of the network system which realizes secure movement of value information.
[Drawing 2]It is the flow chart which showed the procedure for moving value

information to secure one between the IC chips on the network system concerning this embodiment.

[Drawing 3]It is a sequence diagram showing the processing procedure for uploading the value information currently held at the moved material IC chip to SAM12 for movement of each service provider.

[Drawing 4]It is a sequence diagram showing the processing procedure for downloading the value information uploaded to SAM12 for movement of each service provider to a moved material IC chip.

[Drawing 5]It is a figure showing notionally the structure of the radio of the reader/writer and the IC card based on electromagnetic induction.

[Drawing 6]It is the figure which regarded the system which consists of reader/writer and an IC card as one transformerand modeled it.

[Drawing 7]It is a figure showing typically the internal hardware constitutions of the personal digital assistant 110 of the type having IC chip 100.

[Description of Notations]

10 -- Application server (service provider)
11 -- It is usually SAM.
12 -- SAM for movement
20 -- Server for value movement
21 -- Administrative SAM
100 -- IC chip
101 -- Antenna section
102 -- Analog part
103 -- Digital-control part
104 -- Memory
105 -- External interface
110 -- Personal digital assistant
112 -- Indicator
113 -- User input part
114 -- Information storing part
200 -- Reader/writer

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－141429
（P2003－141429A）
(43)公開日　平成15年５月16日(2003.5.16)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	テーマコード（参考）
Ｇ０６Ｆ　17/60	４１０	Ｇ０６Ｆ　17/60	４１０Ｃ　５Ｂ０３５
	５１０		５１０　５Ｂ０５８
	ＺＥＣ		ＺＥＣ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｌ
19/00		19/00	Ｑ

審査請求　未請求　請求項の数21　ＯＬ　（全 16 頁）

(21)出願番号　特願2001－334967(P2001－334967)

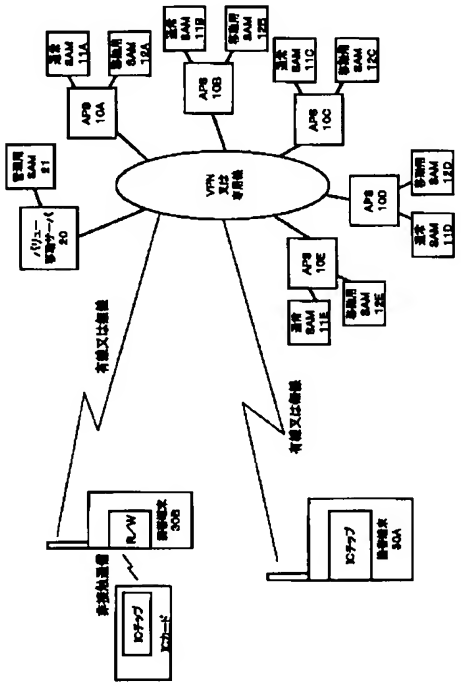
(22)出願日　平成13年10月31日(2001.10.31)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　深田　顕
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大嶋　拓哉
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

Ｆターム(参考)　5B035 AA13 BB09 BC00 BC02 CA29
5B058 CA23 KA31 YA06 YA20

(54)【発明の名称】　データ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体

(57)【要約】
【課題】　複数の価値情報を携帯端末間でセキュアに移動させる。
【解決手段】　バリュー移動用サーバは、ＩＣチップ内の複数の価値情報を、価値情報自体との価値情報にアクセスするために必要な鍵とそのロジックを閉じ込めた、耐タンパ性を持つハードウェア・モジュールＳＡＭを制御して、権限を持つ装置以外には価値情報自体と価値情報にアクセスするために必要な鍵とそのロジックを見せることなく、且つ価値情報の複製や改竄を防止しながら、他のＩＣチップ上にセキュアに移動させる。例えば、携帯端末を新機種に交換する際、一箇所に接続するだけですべての価値情報をセキュアに移動させることができる。



【特許請求の範囲】
【請求項１】価値情報を移動させるためのデータ転送システムであって、
移動対象となる価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置と、
移動元の情報記録媒体に格納された価値情報の前記価値情報サービス装置へのアップロード並びに前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継する価値情報移動サービス装置と、を具備することを特徴とするデータ転送システム。
【請求項２】前記価値情報移動サービス装置は、移動元の情報記録媒体上の価値情報にアクセスするための鍵を通常使用時の本鍵から仮鍵に変更してから前記価値情報サービス装置への価値情報のアップロードを行うとともに、前記価値情報サービス装置から移動先に情報記録媒体上に価値情報をダウンロードした後に仮鍵から本鍵に変更する、ことを特徴とする請求項１に記載のデータ転送システム。
【請求項３】移動元の情報記録媒体上に複数の価値情報が保持され且つ各価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置が複数ある場合には、前記価値情報移動サービス装置は、移動元の情報記録媒体からの価値情報のアップロード並びに移動先の情報記録媒体へのダウンロードを各価値情報サービス装置毎に行う、ことを特徴とする請求項１に記載のデータ転送システム。
【請求項４】前記価値情報移動サービス装置は、価値情報を価値情報サービス装置からダウンロードする前に移動先の情報記録媒体の初期化処理を行う、ことを特徴とする請求項１に記載のデータ転送システム。
【請求項５】前記価値情報移動サービス装置は、移動元の情報記録媒体及び／又は移動先の情報記録媒体を認証処理する、ことを特徴とする請求項１に記載のデータ転送システム。
【請求項６】価値情報を移動させるためのデータ転送方法であって、
移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継するステップと、
価値情報サービス装置が移動中の価値情報を一時的に格納するステップと、前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継するステップと、を具備することを特徴とするデータ転送方法。
【請求項７】価値情報サービス装置へのアップロードを中継する前に移動元の情報記録媒体上の価値情報にアクセスするための鍵を通常使用時の本鍵から仮鍵に変更するステップと、
価値情報サービス装置から移動先に情報記録媒体上に価値情報をダウンロードした後に仮鍵から本鍵に変更するステップと、をさらに備えることを特徴とする請求項６に記載のデータ転送方法。
【請求項８】移動元の情報記録媒体上に複数の価値情報が保持され且つ各価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置が複数ある場合には、前記アップロードを中継するステップ及び／又は前記ダウンロードを中継するステップは各価値情報サービス装置毎に実行する、ことを特徴とする請求項６に記載のデータ転送方法。
【請求項９】価値情報を価値情報サービス装置からダウンロードする前に移動先の情報記録媒体の初期化処理を行うステップをさらに備える、ことを特徴とする請求項６に記載のデータ転送方法。
【請求項１０】移動元の情報記録媒体及び／又は移動先の情報記録媒体を認証処理するステップをさらに備える、ことを特徴とする請求項６に記載のデータ転送方法。
【請求項１１】情報記録媒体間での価値情報の移動をサービスする価値情報移動サービス装置であって、
移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継する手段と、
前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継する手段と、を具備することを特徴とする価値情報移動サービス装置。
【請求項１２】価値情報サービス装置へのアップロードを中継する前に移動元の情報記録媒体上の価値情報にアクセスするための鍵を通常使用時の本鍵から仮鍵に変更する手段と、
価値情報サービス装置から移動先に情報記録媒体上に価値情報をダウンロードした後に仮鍵から本鍵に変更する手段と、をさらに備えることを特徴とする請求項１１に記載の価値情報移動サービス装置。
【請求項１３】移動元の情報記録媒体上に複数の価値情報が保持され且つ各価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置が複数ある場合には、前記アップロードを中継する手段及び／又は前記ダウンロードを中継する手段は各価値情報サービス装置毎に中継を行う、ことを特徴とする請求項１１に記載の価値情報移動サービス装置。
【請求項１４】移動先の情報記録媒体の初期化処理を行う手段をさらに備える、
ことを特徴とする請求項１１に記載の価値情報移動サービス装置。
【請求項１５】移動元の情報記録媒体及び／又は移動先の情報記録媒体を認証処理する手段をさらに備える、こ

とを特徴とする請求項１１に記載の価値情報移動サービス装置。
【請求項１６】情報記録媒体間での価値情報の移動をサービスする価値情報移動サービス方法であって、
移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継するステップと、
前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継するステップと、を具備することを特徴とする価値情報移動サービス方法。
【請求項１７】価値情報サービス装置へのアップロードを中継する前に移動元の情報記録媒体上の価値情報にアクセスするための鍵を通常使用時の本鍵から仮鍵に変更するステップと、
価値情報サービス装置から移動先に情報記録媒体上に価値情報をダウンロードした後に仮鍵から本鍵に変更するステップと、をさらに備えることを特徴とする請求項１６に記載の価値情報移動サービス方法。
【請求項１８】移動元の情報記録媒体上に複数の価値情報が保持され且つ各価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置が複数ある場合には、前記アップロードを中継するステップ及び／又は前記ダウンロードを中継するステップは各価値情報サービス装置毎に実行する、ことを特徴とする請求項１６に記載の価値情報移動サービス方法。
【請求項１９】価値情報を価値情報サービス装置からダウンロードする前に移動先の情報記録媒体の初期化処理を行うステップをさらに備える、ことを特徴とする請求項１６に記載の価値情報移動サービス方法。
【請求項２０】移動元の情報記録媒体及び／又は移動先の情報記録媒体を認証処理するステップをさらに備える、ことを特徴とする請求項１６に記載の価値情報移動サービス方法。
【請求項２１】情報記録媒体間での価値情報の移動をサービスする価値情報移動サービスをコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、
移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継するステップと、
前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継するステップと、を具備することを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを保持するメモリ機能を備えるとともに非接触によりメモリへの読み書きが可能な非接触（又は接触型）ＩＣカード又はＩＣチップに係り、特に、無線データにより外部のリーダ／ライタからメモリ機能へのアクセスを行うための無線インターフェースを備えるとともに、外部機器と接続するための有線インターフェースを備えた非接触ＩＣカード又はＩＣチップ、並びに、有線インターフェースを介してこの種のＩＣカード又はＩＣチップを搭載して用いられる携帯電話機やＰＤＡなどの情報処理端末に関する。
【０００２】更に詳しくは、本発明は、電子マネーや電子チケット、その他の価値情報を電子的に格納した非接触ＩＣカード又はＩＣチップ、並びに、有線インターフェースを介してこの種のＩＣカード又はＩＣチップを搭載して用いられる情報処理端末に係り、特に、情報処理端末間での価値情報のセキュアな移動に関する。
【０００３】
【従来の技術】従来から、本人確認や認証処理のために暗証番号やパスワードを用いたさまざまな装置が考案され、実用に供されている。例えば、銀行やその他の金融機関において、キャッシュ･カードやクレジット・カードを使用する際には、キャッシュ･ディスペンサやその他の金融端末上で、本人認証の手段として、暗証番号やパスワードの入力を使用者に対して促し、使用者から正しい暗証番号やパスワードが入力されたことを確認してから、入出金動作を行なうようになっている。
【０００４】１枚のキャッシュ･カード上に配設されている磁気ストライプなどの記憶媒体の中には、その銀行に対してのみ使用可能な記憶領域しか設けられていない。したがって、上述したような暗証番号あるいはパスワードの入力は、この単一の記憶領域へのアクセスに過ぎないので、偽造や盗用に対する保護は充分とは言い難い。
【０００５】このため、偽造防止などの観点から、キャッシュ・カードやクレジット・カードなどに電気的な接点を持った接触式ＩＣカードや、無線データを介して非接触でデータの読み書きを行う非接触ＩＣカードがよく使われるようになってきている。例えば、キャッシュ･ディスペンサやコンサート会場の出入口、駅の改札口などに設置されたＩＣカード･リーダ／ライタは、利用者がかざしたＩＣカードに非接触でアクセスすることができる。
【０００６】利用者が暗証番号をＩＣカード･リーダ側に入力して、入力された暗証番号をＩＣカード上に格納された暗証番号と照合することで、ＩＣカードとＩＣカード･リーダ／ライタ間で本人確認又は認証処理が行なわれる。そして、本人確認又は認証処理に成功した場合には、例えば、ＩＣカード内に保存されているアプリケーションの利用が可能となる。ここで、ＩＣカードが保持するアプリケーションとしては、例えば、電子マネー

や電子チケットなどの価値情報を挙げることができる。また、前払式証票を電子的に格納することによって、ＩＣカードやこれに接続される携帯端末をプリペイド・カードとして使用することも可能である。（ＩＣカード・アクセス時に使用する暗証番号のことを、特にＰＩＮ（Personalldentification Number）と呼ぶ。）

【０００７】最近では、微細化技術の向上とも相俟って、比較的大容量の記憶空間を持つＩＣカードが出現し、普及してきている。従来のキャッシュ･カードなどにおいては単一の記憶領域すなわち単一のアプリケーションしか担持しないので、各用途又は目的毎に応じた複数のカードを持ち歩く必要がある。これに対して、このような大容量メモリ付きのＩＣカードによれば、複数のアプリケーションを同時に格納しておくことができるので、１枚のＩＣカードを複数の用途に利用することができる。例えば、１枚のＩＣカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケット、デジタル化された前払式証票など、２以上のアプリケーションを格納しておき、１枚のＩＣカードをさまざまな用途に適用させることができる。

【０００８】さらに、ＩＣカードがカード用リーダ／ライタ（カード読み書き装置）との非接触（又は接触型）インターフェースの他に、外部機器と接続するための有線インターフェースを備えることにより、ＩＣカードを携帯電話機、ＰＤＡ（Personal Digital Assistant）に接続したり内蔵して用いることができる（但し、端末に内蔵される多くの場合、ＩＣカードはワンチップ化して構成される）。

【０００９】このような場合、ＩＣカードを利用したさまざまなアプリケーション・サービスを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用いてＩＣカードに対するユーザ・インタラクションを情報処理端末上で行うことができる。また、ＩＣカードが携帯電話機と接続されていることにより、ＩＣカード上に記憶されている内容を電話網を介してやり取りすることもできる。

【００１０】勿論、ＩＣカード上に電子マネーや電子チケット、前払式証票などの価値情報を格納している場合には、情報処理端末は、電子決済、プリペイド・カード様式の決済などの価値情報の処理や、その他のさまざまなサービスを実現することができる。さらに、ＩＣカードとカード読み書き装置間のデータ転送のフェーズに応じた処理や、ＩＣカードの内部状態に応じた処理を提供することができる。

【００１１】ところで、価値情報を格納したＩＣチップが携帯電話機に内蔵される場合などは、機種変更などの理由により、価値情報をＩＣチップ間、すなわち携帯端末間で移動させる必要がある。

【００１２】携帯電話機の機種変更手続は、一般に、電話会社の店舗などで行われ、旧機種内のアドレス帳などの個人情報を新機種に移動してくれる。しかしながら、ＩＣチップ内の価値情報を移動する場合には、移動途中における通信障害やマシン障害などによる価値情報の消失や、価値情報の不法な複製や改竄が行われる可能性があり、電話会社にとっては責任が過大である。

【００１３】そもそも、電話会社は、電子マネーや電子チケットのサービス・プロバイダとは一体ではなく、価値情報にアクセスするために必要な鍵やそのロジックを持たないので、価値情報を処理するには不都合が多い。また、価値情報の移動を請け負うことにより、電話会社には価値情報とその鍵についての責任が必然的に発生する。また、電子マネーや電子チケットのサービス・プロバイダにとっては、サービスの信用の根幹となるアクセス鍵やそのロジックを、電話会社とはいえ、外部に渡すことは好ましくない。

【００１４】価値情報のサービス・プロバイダは、通常、耐タンパ性を持つハードウェア・モジュールＳＡＭ（Secure Application Module）を用いて、価値情報自体と価値情報にアクセスするための鍵、並びにそのロジックを閉じ込めている。電話会社などの１箇所の移動用サーバにより複数の価値情報を移動させるには、一時的であれ価値情報を保存する必要があるが、ＳＡＭのようなものを利用しない限り、この移動用サーバにより独自に暗号化したとしても、価値情報やその鍵をサーバ上で解読されてしまう可能性が高くなる。

【００１５】これに対し、携帯端末本体の機種変更手続とは別に、ＩＣチップ内の価値情報の移動をその価値情報のサービス・プロバイダによって行うという方法も考えられる。この方法は責任分離という観点からは有効であろう。

【００１６】しかしながら、ユーザは携帯端末の機種変更に伴い、複数の手続を取らなければならない。特に、ＩＣカードやＩＣチップのメモリ容量の増大に伴い、１つのＩＣチップ内に多種類の価値情報が格納されているような場合には、それぞれのサービス・プロバイダに対して価値情報の移動手続を取らなければならず、極めて煩わしい。また、ＩＣチップから価値情報を読み出すリーダ／ライタは、複数のサービス・プロバイダへセッションを切り換える必要があるが、この切り換え操作を手動で行うには手間がかかる。また、ＩＣチップ側の通信の仕組みも複雑になるので障害が発生する可能性が高くなる。

【００１７】

【発明が解決しようとする課題】本発明の目的は、電子マネーや電子チケットなどの価値情報をセキュアに移動させることができる、優れたデータ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体を提供することにあ

る。

【００１８】本発明の更なる目的は、ＩＣカードやＩＣチップ内に保持されている電子マネーや電子チケットなどの価値情報をセキュアに移動させることができる、優れたデータ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体を提供することにある。

【００１９】本発明の更なる目的は、ＩＣカードやＩＣチップ内に保持されている複数の価値情報を、１箇所のサーバに接続するだけでセキュアに移動させることができる、優れたデータ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体を提供することにある。

【００２０】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、価値情報を移動させるためのデータ転送システムであって、移動対象となる価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置と、移動元の情報記録媒体に格納された価値情報の前記価値情報サービス装置へのアップロード並びに前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継する価値情報移動サービス装置と、を具備することを特徴とするデータ転送システムである。

【００２１】但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

【００２２】また、本発明の第２の側面は、価値情報を移動させるためのデータ転送方法であって、移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継するステップと、価値情報サービス装置が移動中の価値情報を一時的に格納するステップと、前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継するステップと、を具備することを特徴とするデータ転送方法である。

【００２３】本発明の第１又は第２の側面に係るデータ転送システム又はデータ転送方法によれば、ＩＣチップなどの情報記録媒体に保持されている価値情報を、価値情報自体との価値情報にアクセスするために必要な鍵とそのロジックを閉じ込めた、耐タンパ性を持つハードウェア・モジュールＳＡＭなどの価値情報サービス装置を制御して、権限を持つ装置以外には価値情報自体と価値情報にアクセスするために必要な鍵とそのロジックを見せることなく、且つ価値情報の複製や改竄を防止しながら、他の情報記録媒体上にセキュアに移動させることができる。例えば、携帯端末を新機種に交換する際、一箇所に接続するだけで端末内に保持されているすべての価値情報をセキュアに移動させることができる。したがって、価値情報の移動事業者と、価値情報サービスを運用する各サービス・プロバイダの責任範囲を明確に分離することができる。

【００２４】ここで、前記価値情報移動サービス装置は、移動元の情報記録媒体上の価値情報にアクセスするための鍵を通常使用時の本鍵から仮鍵に変更してから前記価値情報サービス装置への価値情報のアップロードを行うようにしてもよい。このような場合、移動の途中で価値情報が不正に複製や改竄されて使用されることを防ぐことができる。また、価値情報の移動に失敗した場合であっても、移動元の鍵を本鍵に戻すことによりバックアップとして用いることができ、価値情報の消失を防ぐことができる。

【００２５】また、前記価値情報移動サービス装置は、前記価値情報サービス装置から移動先に情報記録媒体上に価値情報をダウンロードした後に仮鍵から本鍵に変更するようにしてもよい。このような場合、移動元の情報記録媒体に残されている価値情報を仮鍵のままとすることにより通常使用を不能のままとなるので、不正使用を防ぐことができる。

【００２６】また、移動元の情報記録媒体上に複数の価値情報が保持され且つ各価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置が複数ある場合には、前記価値情報移動サービス装置は、移動元の情報記録媒体からの価値情報のアップロード並びに移動先の情報記録媒体へのダウンロードを各価値情報サービス装置毎に行うようにしてもよい。このような場合、１箇所の価値情報移動サービス装置に接続すればよく、手動又は自動で価値情報サービス毎に通信を逐次切り換える必要がない。このため、手間が減り、通信障害が起こる可能性を減少させることができる。移動元の情報記録媒体側から考えると、中継先となる個々の価値情報サービス装置を意識する必要がなく、手続が簡素化される。

【００２７】前記価値情報移動サービス装置は、価値情報を価値情報サービス装置からダウンロードする前に移動先の情報記録媒体の初期化処理を行うようにしてもよい。

【００２８】また、前記価値情報移動サービス装置は、移動元の情報記録媒体及び／又は移動先の情報記録媒体を認証処理するようにしてもよい。

【００２９】また、本発明の第３の側面は、情報記録媒体間での価値情報の移動をサービスする価値情報移動サービス装置又は価値情報移動サービス方法であって、移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継する手段又はステップと、前記価値情報サービス装置から

移動先の情報記録媒体への価値情報のダウンロードを中継する手段又はステップと、を具備することを特徴とする価値情報移動サービス装置又は価値情報移動サービス方法である。

【００３０】本発明の第３の側面に係る価値情報移動サービス装置又は価値情報移動サービス方法によれば、ＩＣチップなどの情報記録媒体に保持されている価値情報を、価値情報自体との価値情報にアクセスするために必要な鍵とそのロジックを閉じ込めた、耐タンパ性を持つハードウェア・モジュールＳＡＭなどの価値情報サービス装置を制御して、権限を持つ装置以外には価値情報自体と価値情報にアクセスするために必要な鍵とそのロジックを見せることなく、且つ価値情報の複製や改竄を防止しながら、他の情報記録媒体上にセキュアに移動させることができる。例えば、携帯端末を新機種に交換する際、一箇所に接続するだけで端末内に保持されているすべての価値情報をセキュアに移動させることができる。したがって、携帯端末の機種切り換えを行う事業者は、価値情報サービスを運用する各サービス・プロバイダの責任範囲を明確に分離しながら価値情報の移動を行うことができる。

【００３１】ここで、本発明の第３の側面に係る価値情報移動サービス装置は、移動元の情報記録媒体上の価値情報にアクセスするための鍵を通常使用時の本鍵から仮鍵に変更してから前記価値情報サービス装置への価値情報のアップロードを行うようにしてもよい。このような場合、移動の途中で価値情報が不正に複製や改竄されて使用されることを防ぐことができる。また、価値情報の移動に失敗した場合であっても、移動元の鍵を本鍵に戻すことによりバックアップとして用いることができ、価値情報の消失を防ぐことができる。

【００３２】また、前記価値情報サービス装置から移動先に情報記録媒体上に価値情報をダウンロードした後に仮鍵から本鍵に変更するようにしてもよい。このような場合、移動元の情報記録媒体に残されている価値情報を仮鍵のままとすることにより通常使用を不能のままとなるので、不正使用を防ぐことができる。

【００３３】また、移動元の情報記録媒体上に複数の価値情報が保持され且つ各価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置が複数ある場合には、移動元の情報記録媒体からの価値情報のアップロード並びに移動先の情報記録媒体へのダウンロードを各価値情報サービス装置毎に行うようにしてもよい。このような場合、１箇所の価値情報移動サービス装置に接続すればよく、手動又は自動で価値情報サービス毎に通信を逐次切り換える必要がない。このため、手間が減り、通信障害が起こる可能性を減少させることができる。移動元の情報記録媒体側から考えると、中継先となる個々の価値情報サービス装置を意識する必要がなく、手続が簡素化される。

【００３４】本発明の第３の側面に係る価値情報移動サービス装置又は価値情報移動サービス方法は、価値情報を価値情報サービス装置からダウンロードする前に移動先の情報記録媒体の初期化処理を行うようにしてもよい。

【００３５】また、本発明の第３の側面に係る価値情報移動サービス装置又は価値情報移動サービス方法は、移動元の情報記録媒体及び／又は移動先の情報記録媒体を認証処理するようにしてもよい。

【００３６】また、本発明の第４の側面は、情報記録媒体間での価値情報の移動をサービスする価値情報移動サービスをコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、移動元の情報記録媒体から価値情報自体と価値情報にアクセスするための鍵とそのロジックを安全に保持する価値情報サービス装置への価値情報のアップロードを中継するステップと、前記価値情報サービス装置から移動先の情報記録媒体への価値情報のダウンロードを中継するステップと、を具備することを特徴とする記憶媒体である。

【００３７】本発明の第４の側面に係る記憶媒体は、例えば、様々なプログラム･コードを実行可能な汎用コンピュータ･システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、ＤＶＤ（Digital Versatile Disc）やＣＤ（Compact Disc）、ＦＤ（Floppy Disk）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

【００３８】本発明の第４の側面に係る記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第４の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第３の側面に係る価値情報移動サービス装置又は価値情報移動サービス方法と同様の作用効果を得ることができる。

【００３９】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４０】

【発明の実施の形態】以下、図面を参照しながら本発明の実施形態について詳解する。

【００４１】本発明は、ＩＣカードやＩＣチップ内に保持されている複数の価値情報を、１箇所のサーバに接続するだけでセキュアに移動させるものである。価値情報の移動を行うサーバのことを、以下では「バリュー移動サーバ」と呼ぶことにする。例えば、携帯電話機の機種変更の際に、内蔵されたＩＣチップ上の価値情報を移動するような場合、機種変更サービスを行う電話会社などがバリュー移動サーバを運営すればよい。バリュー移動サーバは、個々の価値情報サービスのプロバイダとは一体化されている訳ではないが、本発明によれば、価値情報の移動をセキュアに行うことができるので、責任の分離が明確となり、バリュー移動サーバを運営する事業者の責任が過大となることはない。

【００４２】図１には、価値情報のセキュアな移動を実現するネットワーク・システムの構成を模式的に示している。

【００４３】同図に示すように、ＶＰＮ（Virtual Private Network）あるいは専用線などのネットワーク上には、電子マネーや電子チケットなどの価値情報サービスを行うプロバイダが設置するアプリケーション・サーバ（ＡＰＳ）１０Ａ，１０Ｂ…と、ＩＣカードやＩＣチップに内蔵された価値情報をＩＣチップ間でセキュアに移動させるためのバリュー移動サーバ２０が存在する。

【００４４】各アプリケーション・サーバ（ＡＰＳ）１０Ａ，１０Ｂ…、並びに、バリュー移動用サーバ２０は、それぞれ耐タンパ性を持つハードウェア・モジュールＳＡＭ（Secure Application Module）を備えている。ＳＡＭは、価値情報自体と価値情報にアクセスするための鍵、並びにそのロジックを閉じ込めている。

【００４５】本実施形態では、バリュー移動用サーバ２０は、各ＩＣチップ内の情報をセキュアに管理するために管理用ＳＡＭ２１を備えている。管理用ＳＡＭ２１は、ＩＣチップの初期化処理など、価値情報を保持している各ＩＣチップの管理を行う。また、管理用ＳＡＭ２１は、ＩＣチップ内の価値情報を移動する際に、通常使用時の「本鍵」から移動時のみ使用する一時的な「仮鍵」に変更するためのロジックを備えている。

【００４６】また、各アプリケーション・サーバ１０Ａ…は、価値情報を通常使用する際に用いる本鍵で動作する通常ＳＡＭ１１と、バリュー移動用サーバ２０の管理用ＳＡＭ２１が発行する仮鍵によって移動時に動作する移動用ＳＡＭ１２を備えている。

【００４７】通常ＳＡＭ１１は、各サービス・プロバイダアプリケーション・サーバ１０上で個別に管理され、価値情報のサービスを行う。通常ＳＡＭ１１は、価値情報にアクセスする鍵とそのロジックを知る各サービス・プロバイダがそれぞれの他者は権限を持たない限り、通常ＳＡＭ１１の中を知ることができない。バリュー移動用サーバ２０も、通常ＳＡＭ１１の中身を知ることができない。

【００４８】通常ＳＡＭ１１と移動用ＳＡＭ１２は、物理的には、同じハードウェア・モジュール内で一体化されていても、個々に独立したハードウェア・モジュールであってもよい。また、契約などにより、サービス・プロバイダは、自身が運営するアプリケーション・サーバではなくバリュー移動用サーバ２０など別の場所にＳＡＭを配置していてもよい。

【００４９】各アプリケーション・サーバ１０やバリュー移動用サーバ２０は、専用のハードウェアによりサーバ装置として構成することも可能であるが、ワークステーション（ＷＳ）やパーソナル・コンピュータ（ＰＣ）と呼ばれる一般的な計算機システム上で所定のサーバ・アプリケーションを起動するという形態でも実現することができる。計算機システムの一例は、米ＩＢＭ社のＰＣ／ＡＴ互換機又はその後継機である。

【００５０】また、ＩＣカードは、ＩＣチップとして携帯電話機やＰＤＡ（Personal Digital Assistant）などの携帯端末３０Ａに内蔵して用いられているか、あるいは、リーダ／ライタ付きの携帯端末３０Ｂに非接触（又は接触）アクセスして用いられる。携帯端末の機種変更やＩＣカード自体の交換のために、ＩＣチップ又はＩＣカード間で価値情報を移動する場合には、携帯端末３０は、無線又は有線の通信媒体を介してＶＰＮに接続して、バリュー移動サーバ２０に価値情報の移動を依頼する。本実施形態では、ＩＣチップに保持された複数の価値情報を移動する場合であっても、携帯端末３０は、一箇所のバリュー移動サーバ２０に接続するだけでよい、という点に充分留意されたい。

【００５１】バリュー移動用サーバ２０は、価値情報の移動に際し、管理用ＳＡＭ２１を使用して、ＩＣチップを通信路経由で制御する。

【００５２】本実施形態では、バリュー移動用サーバ２０は、管理用ＳＡＭ２１を用いて、価値情報の移動のために各サービス・プロバイダの移動用ＳＡＭ１２とＩＣチップ間で暗号化通信が行われる際、それを中継する役割を担う。また、ＩＣチップ側のリーダ／ライタ機能を持つ携帯端末３０ＢやＩＣチップ内蔵型の携帯端末３０Ａは、ＳＡＭとＩＣチップ間で暗号化通信が行われる際、ＩＣチップとバリュー移動サーバ２０との接続を行なう役割を担う。

【００５３】バリュー移動用サーバ２０と各移動用ＳＡＭ１２との間は、バリュー移動用サーバ２０がある移動用ＳＡＭ１２を制御する権限についてそれぞれ個別に設定可能とする。また、バリュー移動用サーバ２０と各移動用ＳＡＭ１２との間は、ＰＫＩ（Public Key Infrastructure：公開鍵暗号基盤）若しくは共通鍵による暗号化が可能である。また、バリュー移動用サーバ２０と遠隔の移動用ＳＡＭ１２との間には、ＶＰＮ又は専用線で接続されている。

【００５４】図１に示したネットワーク・システムにお

いて、ＩＣカード又は携帯端末に内蔵されたＩＣチップ内の価値情報を移動するためには、移動元並びに移動先となるＩＣチップの接続先は、単一のバリュー移動用サーバ２０となる。

【００５５】バリュー移動用サーバ２０の管理用ＳＡＭ２１は、価値情報を移動する前に、価値情報の鍵を通常使用時の「本鍵」から移動のための一時的な「仮鍵」に変更する。また、ＩＣチップ内に保持されているすべての価値情報の移動が完了しないうちは、元のＩＣチップの位置情報をまだ削除せず、バックアップ用として保持しておく。

【００５６】移動が完了したときには、管理用ＳＡＭ２１は移動先のＩＣチップにおいて仮鍵を本鍵に戻すことにより、価値情報の通常使用が可能となる。また、バックアップ用に残しておいた移動元のＩＣチップ側に関しては仮鍵のままとすることにより通常使用を不能のままとなるので、不正使用を防ぐことができる。

【００５７】バリュー移動用サーバ２０は、ＩＣチップ内の個々の価値情報を、該当するサービス・プロバイダの移動用ＳＡＭ１２を用いて移動を行う。この際、サービス・プロバイダ（ＡＰＳ）側の移動用ＳＡＭ１２では、事前にバリュー移動用サーバ２０からのアクセス制限を設定する。

【００５８】サービス・プロバイダのアプリケーション・サーバ１０側では、通常使用時に価値情報にアクセスするための鍵と、そのロジックを通常ＳＡＭ１１に格納するとともに、価値情報移動用の鍵やそのロジックを移動用ＳＡＭ１２に格納している。また、移動時に、ＩＣチップ内の価値情報は、アプリケーション・サーバ１０の移動用ＳＡＭ１２内に一時的に保存される。

【００５９】価値情報の移動先となるＩＣチップ側では、そのメモリ領域のフォーマッティングなどの所定の前処理を行った後、バリュー移動用サーバ２０経由で、サービス・プロバイダすなわちアプリケーション・サーバ１０の移動用ＳＡＭ１２から価値情報をダウンロードすることで、その移動が完了する。

【００６０】移動後は、管理用ＳＡＭ２１が正しい鍵に変えることによって、以後同じ移動用の鍵で価値情報を移動することを不能にする。この結果、移動元のＩＣチップ上に残っているバックアップ用の価値情報は使用できなくなる。

【００６１】そして、ＩＣチップ内のすべての価値情報の移動が完了すると、サービス・プロバイダの移動用ＳＡＭ１２内に一時的に保存されていた価値情報を削除する。

【００６２】図２には、本実施形態に係るネットワーク・システム上で、ＩＣチップ間で価値情報をセキュアに移動させるための処理手順をフローチャートの形式で示している。この処理手順は、携帯端末を介してネットワーク接続されるＩＣチップと、バリュー移動用サーバ２０と、該当する各アプリケーション・サーバ（プロバイダ）１０の移動用ＳＡＭ１２間での協働的な動作により実現される。以下、このフローチャートを参照しながら、価値情報のセキュアな移動処理について説明する。

【００６３】まず、価値情報の移動元となるＩＣチップは、リーダ／ライタ機能を持つ通信装置（例えばリーダ／ライタ付きの携帯電話機、又はＩＣチップ内蔵の携帯電話機）３０と接続する。さらに、移動元のＩＣチップは、この通信装置３０経由でバリュー移動用サーバ２０と接続して、通信装置３０から送られるユーザＩＤ、パスワードでバリュー移動用サーバ２０と認証する（ステップＳ１）。

【００６４】バリュー移動用サーバ２０は、価値情報の移動元ＩＣチップ内を検索して、そのＩＣチップ内に登録されているすべての価値情報の種類を検知するとともに、それらの情報をサーバ２０ローカルの移動情報データベース（図示しない）に保存する。あるいは、バリュー移動用サーバ２０側が事前に用意したＩＣチップのシリアル・ナンバーとその登録している価値情報の種類の対照テーブルを事前に移動情報データベース内に用意しておき、価値情報の移動元ＩＣチップのシリアル・ナンバーを得ることにより、この対照テーブルを利用して、ＩＣチップ内に登録されている価値情報の種類をつきとめる（ステップＳ２）。価値情報の種類毎に、対応するサービス・プロバイダすなわちＳＡＭを用意するアプリケーション・サーバが異なるものとする。

【００６５】次いで、バリュー移動用サーバ２０の管理用ＳＡＭ２１は、価値情報の移動元ＩＣチップ内の価値情報自体にアクセスするために必要な鍵を、通常使用時の「本鍵」から、移動時に一時的に使用する「仮鍵」に変更する（ステップＳ３）。この結果、価値情報の移動中に移動元ＩＣチップ上では、通常の価値情報の利用が不可能な状態となる。すなわち、仮鍵に切り換わることにより、該当するサービス・プロバイダの通常ＳＡＭ１１はＩＣチップ内の価値情報にアクセスできなくなる代わりに、移動用ＳＡＭ１２がＩＣチップ内の価値情報へのアクセスが可能になる。

【００６６】次いで、バリュー移動用サーバ２０は、ＩＣチップ内から検索されたサービス・プロバイダを１つ取り出す（ステップＳ４）。そして、バリュー移動用サーバ２０の管理用ＳＡＭ２１は、価値情報の種類単位（アプリケーション単位）で価値情報の移動を開始する。

【００６７】まず、最初に移動させる価値情報を管理するサービス・プロバイダすなわちアプリケーション・サーバ１０の移動用ＳＡＭ１２を特定して、価値情報の移動元のＩＣチップをその移動用ＳＡＭ１２と通信させる（ステップＳ５）。

【００６８】バリュー移動元のＩＣチップは、当該チップ内のある価値情報に関して、チップ内にある鍵で移動用ＳＡＭ１２と相互認証を行い、暗号化通信を始める

（ステップＳ６）。

【００６９】次いで、価値情報の移動元ＩＣチップ内の価値情報を、アプリケーション・サーバ１０側の移動用ＳＡＭ１２内のメモリ・エリアにコピー（すなわち、価値情報のアップロード）する（ステップＳ７）。

【００７０】価値情報の移動用ＳＡＭ１２内のメモリ・エリアへのコピーが終了すると、次の移動対象価値情報を管理するサービス・プロバイダの移動用ＳＡＭ１２を特定して、上述と同様の手順により、移動元ＩＣチップをその移動用ＳＡＭ１２と通信させる。引き続き、移動元ＩＣチップ内のすべての価値情報のコピーすなわちアップロードが終わるまで、ステップＳ４、Ｓ５、Ｓ６、及びＳ７を繰り返す（ステップＳ８）。

【００７１】言い換えれば、価値情報の移動元ＩＣチップが接続するバリュー移動用サーバ２０は１箇所であり、このバリュー移動用サーバ２０は、移動元のＩＣチップとサービス・プロバイダの各移動用ＳＡＭ１２との通信を言わば中継する。

【００７２】移動元ＩＣチップ内のすべての価値情報をそれぞれのサービス・プロバイダの移動用ＳＡＭ１２へのコピーが完了した後、すなわち価値情報のアップロードが完了した後、今度は、価値情報の移動先ＩＣチップが接続されたリーダ／ライタ機能を持つ通信装置（例えばリーダ／ライタ機能を持つ携帯電話機や、ＩＣチップを内蔵する携帯電話機）３０は、バリュー移動用サーバ２０と接続して、通信装置から送られるユーザＩＤ、パスワードでバリュー移動用サーバ２０と認証する（ステップＳ９）。

【００７３】バリュー移動用サーバ２０の管理用ＳＡＭ２１は、価値情報の移動先ＩＣチップとの認証情報により、移動情報データベースを検索して、この移動先ＩＣチップの初期化(フォーマット)情報を得る。そして、バリュー移動用サーバ１０の管理用ＳＡＭ２１は、この初期化情報に基づき、移動先ＩＣチップのメモリ・エリアを初期化する（ステップＳ１０）。この初期化に際して、価値情報の使用時に使う本鍵ではなく、価値情報移動用の仮鍵を用いる。

【００７４】次いで、バリュー移動用サーバ２０は、移動情報データベースからサービス・プロバイダを１つ取り出す（ステップＳ１１）。そして、バリュー移動用サーバ２０は、価値情報の種類単位(アプリケーション単位)で価値情報の移動すなわちＩＣチップへのダウンロードを開始する。

【００７５】まず、最初に移動させる価値情報を管理するサービス・プロバイダすなわちアプリケーション・サーバの移動用ＳＡＭ１２を特定して、価値情報の移動先のＩＣチップをその移動用ＳＡＭ１２と通信させる（ステップＳ１２）。

【００７６】そして、価値情報の移動先のＩＣチップはある価値情報に関して、初期化時にセットされたチップ内の鍵すなわち仮鍵を使用して、移動用ＳＡＭ１２と相互認証を行い、暗号化通信を始める（ステップＳ１３）。

【００７７】次いで、移動用ＳＡＭ１２内のメモリ・エリアに価値情報の移動元ＩＣチップ内からコピーすなわちアップロードされた価値情報を、価値情報の移動先ＩＣチップ内にコピーすなわちダウンロードする（ステップＳ１４）。

【００７８】ある価値情報についての移動先ＩＣチップ内へのコピーが終了すると、次に移動対象となる価値情報を管理するサービス・プロバイダの移動用ＳＡＭ１２を特定して、上述と同様の手順により、移動先ＩＣチップをその移動用ＳＡＭ１２と通信させる。引き続き、移動先ＩＣチップ内へのすべての価値情報のコピーが終わるまで、ステップＳ１１、Ｓ１２、Ｓ１３、及びＳ１４を繰り返す（ステップＳ１５）。

【００７９】言い換えれば、価値情報の移動先ＩＣチップが接続するバリュー移動用サーバ２０は１箇所であり、このバリュー移動用サーバ２０は、移動先のＩＣチップと各サービス・プロバイダの移動用ＳＡＭ１２との通信を言わば中継する。

【００８０】すべての価値情報の移動が完了すると、バリュー移動用サーバ２０は、バリュー移動先ＩＣチップの価値情報移動用の仮鍵を、通常使用時の本鍵に変更する（ステップＳ１６）。この結果、移動先のＩＣチップ側では、価値情報の通常使用が可能となる。また、バックアップ用に残しておいたＩＣチップに関しては仮鍵のままとすることにより通常使用を不能のままとなるので、不正使用を防ぐことができる。また、必要に応じて、移動元のＩＣチップ内に残されたままの価値情報を削除する。

【００８１】さらに、バリュー移動用サーバ２０は、価値情報の移動に関係したそれぞれのアプリケーション・サーバ１０の移動用ＳＡＭ２１内のメモリ・エリアに保存しておいた移動用価値情報をクリアする（ステップＳ１７）。

【００８２】図３には、移動元ＩＣチップに保持されている価値情報を個々のサービス・プロバイダの移動用ＳＡＭ１２にアップロードするための処理手続きを示している。以下、同図を参照しながら、価値情報を移動元ＩＣチップから移動用ＳＡＭ１２にアップロードするための各者間の協働的動作について説明する。

【００８３】まず、価値情報の移動元となるＩＣチップは、リーダ／ライタ機能を持つ通信装置（例えばリーダ／ライタ付きの携帯電話機、又はＩＣチップ内蔵の携帯電話機）３０と接続して、通信装置はＩＣチップのシリアル・ナンバーなどを取得する。

【００８４】次いで、リーダ／ライタ機能を持つ通信装置は、バリュー移動用サーバ２０との間でユーザ認証を行い、認証に成功した後、この通信装置にＩＣチップ・

コントロール用の通信路の確保を要求し、通信路が確保される。

【００８５】次いで、バリュー移動用サーバ２０は、管理用ＳＡＭ２１に対して移動元ＩＣチップ内の価値情報自体にアクセスするために必要な鍵を、通常使用時の「本鍵」から、移動時に一時的に使用する「仮鍵」に変更するよう、鍵変更を依頼し、管理用ＳＡＭ２１はこの鍵変更処理を行う。本鍵から仮鍵に変更されたことにより、該当するサービス・プロバイダ１０側では通常ＳＡＭ１１ではなく移動用ＳＡＭ１２が移動元ＩＣチップの価値情報にアクセスできるようになる。

【００８６】次いで、バリュー移動用サーバ２０は、価値情報を管理するサービス・プロバイダ１０に対して、価値情報の移動（アップロード）処理を依頼する。

【００８７】サービス・プロバイダ１０側では、この価値情報移動処理の依頼に応答して、移動用ＳＡＭ１２が、移動元ＩＣチップに対して価値情報のアップロード依頼を発行する。これに対して、移動元ＩＣチップは、価値情報を移動用ＳＡＭ１２にコピーすなわちアップロードを行う。

【００８８】価値情報移動処理依頼、価値情報アップロード依頼、並びに価値情報のアップロードは、必要なサービス・プロバイダの分だけ繰り返し実行する。

【００８９】また、図４には、サービス・プロバイダの移動用ＳＡＭ１２にアップロードされている価値情報を移動先のＩＣチップにダウンロードするための処理手続きを示している。以下、同図を参照しながら、価値情報を移動用ＳＡＭ１２から移動先ＩＣチップにダウンロードするための各者間の協働的動作について説明する。

【００９０】まず、価値情報の移動元となるＩＣチップは、リーダ／ライタ機能を持つ通信装置（例えばリーダ／ライタ付きの携帯電話機、又はＩＣチップ内蔵の携帯電話機）３０と接続して、通信装置はＩＣチップのシリアル・ナンバーなどを取得する。

【００９１】次いで、リーダ／ライタ機能を持つ通信装置は、バリュー移動用サーバ２０との間でユーザ認証を行い、認証に成功した後、この通信装置にＩＣチップ・コントロール用の通信路の確保を要求し、通信路が確保される。

【００９２】通信路が確保されると、バリュー移動用サーバ２０の管理用ＳＡＭ２１は、移動先ＩＣチップのシリアル・ナンバーにより移動情報データベースを検索して、この移動先ＩＣチップの初期化（フォーマット）情報を得る。そして、バリュー移動用サーバ１０の管理用ＳＡＭ２１は、この初期化情報に基づき、移動先ＩＣチップのメモリ・エリアを初期化する。移動先ＩＣチップは、初期化が終了するとこれを管理用ＳＡＭ２１に通知する。

【００９３】次いで、バリュー移動用サーバ２０は、価値情報を管理するサービス・プロバイダ１０に対して、価値情報の移動（ダウンロード）処理を依頼する。

【００９４】サービス・プロバイダ１０側では、この価値情報移動処理の依頼に応答して、移動用ＳＡＭ１２が、自身のメモリ・エリアにアップロードされている価値情報を移動先のＩＣチップにダウンロードする。これに対して、移動先のＩＣチップは、ダウンロードが完了するとこれを通知する。

【００９５】価値情報移動処理依頼、価値情報ダウンロード依頼、並びに価値情報のダウンロード終了通知は、必要なサービス・プロバイダの分だけ繰り返し実行する。

【００９６】そして、すべての価値情報のダウンロードが完了すると、バリュー移動用サーバ２０は、管理用ＳＡＭ２１に対して移動先ＩＣチップ内の価値情報自体にアクセスするために必要な鍵を、通常使用時の「仮鍵」から、移動時に一時的に使用する「本鍵」に変更するよう、鍵変更を依頼し、管理用ＳＡＭ２１はこの鍵変更処理を行う。仮鍵から本鍵に戻されたことにより、該当するサービス・プロバイダ１０側では移動用ＳＡＭ１２ではなく通常ＳＡＭ１１が移動元ＩＣチップの価値情報にアクセスできるようになる。

【００９７】この結果、移動先のＩＣチップでは、価値情報の通常使用（例えば、電子マネーによる電子決済や電子チケットの使用など）が可能となる。一方、バックアップ用に残しておいた移動元のＩＣチップ側に関しては仮鍵のままとすることにより通常使用を不能のままとなるので、不正使用を防ぐことができる。また、必要に応じて、移動元のＩＣチップ内に残されたままの価値情報を削除する。

【００９８】図５及び図５には、ＩＣカードとカード・リーダ／ライタ間における非接触データ通信の仕組みを図解している。

【００９９】リーダ／ライタとＩＣカード間の無線通信は、例えば電磁誘導の原理に基づいて実現される。図５には、電磁誘導に基づくリーダ／ライタとＩＣカードとの無線通信の仕組みを概念的に図解している。リーダ／ライタは、ループ･コイルで構成されたアンテナL_{RW}を備え、このアンテナL_{RW}に電流I_{RW}を流すことでその周辺に磁界を発生させる。一方、ＩＣカード側では、電気的にはＩＣカードの周辺にループ･コイルL_Cが形設されている。ＩＣカード側のループ･コイルL_C端にはリーダ／ライタ側のループ・アンテナL_Cが発する磁界による誘導電圧が生じ、ループ･コイルL_C端に接続されたＩＣカードの端子に入力される。

【０１００】リーダ／ライタ側のアンテナL_{RW}とＩＣカード側のループ･コイルL_Cは、その結合度は互いの位置関係によって変わるが、系としては１個のトランスを形成していると捉えることができ、図６に示すようにモデル化することができる。

【０１０１】リーダ／ライタ側では、アンテナL_{RW}に流

す電流I_{RW}を変調することで、ＩＣチップ上のループ・コイルL_Cに誘起される電圧V_0は変調を受け、そのことを利用してリーダ／ライタはＩＣカードへのデータ送信を行うことができる。

【０１０２】また、ＩＣカードは、リーダ／ライタへ返送するためのデータに応じてループ・コイルL_Cの端子間の負荷を変動させる機能（Load Switching）を持つ。ループ・コイルL_Cの端子間の負荷が変動すると、リーダ／ライタ側ではアンテナ端子間のインピーダンスが変化して、アンテナL_{RW}の通過電流I_{RW}や電圧V_{RW}の変動となって現れる。この変動分を復調することで、リーダ／ライタはＩＣカードの返送データを受信することができる。

【０１０３】すなわち、ＩＣカードは、リーダ／ライタからの質問信号に対する応答信号に応じて自身のアンテナ間の負荷を変化させることによって、リーダ／ライタ側の受信回路に現れる信号に振幅変調をかけて通信を行うことができる。

【０１０４】また、図７には、ＩＣチップ１００を内蔵したタイプの携帯端末１１０の内部ハードウェア構成を模式的に示している。ここで言う携帯端末１１０には、携帯電話機やＰＤＡ（Personal Digital Assistant）などの情報処理端末に相当する。携帯電話機であれば、無線電話網経由でＶＰＮ又は専用線に接続される。また、携帯端末であれば、他の携帯電話機を介して無線電話網経由でＶＰＮ又は専用線に接続される。

【０１０５】同図に示すように、ＩＣチップ１００は、アンテナ部１０１と、アナログ部１０２と、ディジタル制御部１０３と、メモリ１０４と、外部インターフェース１０５とで構成されている。

【０１０６】アンテナ部１０１は、リーダ／ライタ２００との間で非接触データの送受信を行う。アナログ部１０２は、検波、変復調、クロック抽出など、アンテナ部１０１から送受信されるアナログ信号の処理を行う。ＩＣチップ１００は、リーダ／ライタ２００からの質問信号に対する応答信号に応じて自身のアンテナ間の負荷を変化させることによって、リーダ／ライタ側の受信回路に現れる信号に振幅変調をかけて通信を行うことができる。

【０１０７】ディジタル制御部１０３は、送受信データの処理やその他ＩＣカード内の動作を統括的にコントロールする。ディジタル制御部１０３は、アドレス可能なメモリ１０４をローカルに接続しており、電子マネーや電子チケットなどのアプリケーションを格納したり、ディジタル制御部１０３が実行するプログラム・コードをロードしたり、実行中の作業データを保存するために使用することができる。

【０１０８】ＩＣチップ１００のメモリ１０４には、さまざまなアプリケーションが格納されている。アプリケーションとしては、例えば、電子マネーや電子チケットなどの価値情報を挙げることができる。

【０１０９】外部インターフェース１０５は、リーダ／ライタ２００とを結ぶ非接触インターフェースとは相違するインターフェース・プロトコルにより、ディジタル制御部１０３が携帯端末１１０本体と接続するための機能モジュールである。メモリ１０４に書き込まれたデータは、外部インターフェース１０５を経由して、携帯端末１１０本体側に転送することができる。

【０１１０】本実施形態では、携帯端末１１０と内蔵ＩＣチップ１００を接続する外部インターフェース１０５には、ＵＡＲＴやI^2Cのような有線インターフェースを使用する。但し、外部インターフェース１０５のインターフェース仕様は特に限定されず、他の有線インターフェースであっても、あるいはＢｌｕｅｔｏｏｔｈやＩＥＥＥ．８０２．１１ｂなどの無線インターフェースであってもよい。

【０１１１】ＩＣチップ１００は、例えば、アンテナ部１０１経由で受信されるカード読み書き装置からの受信電波によって駆動することができる。勿論、携帯端末１１０側からの供給電力によって、一部又は全部が動作するように構成されていてもよい。

【０１１２】一方、携帯端末１１０本体側は、プログラム制御部１１１と、表示部１１２と、ユーザ入力部１１３とで構成される。

【０１１３】プログラム制御部１１１は、例えばマイクロプロセッサと、ＲＡＭと、ＲＯＭで構成され（いずれも図示しない）、マイクロプロセッサは、ＲＯＭに格納されたプログラム・コードに従って、ＲＡＭを作業領域に用いてさまざまな処理サービスを実行する。処理サービスには、携帯電話機やＰＤＡなどの携帯端末１１０本来の機能の他に、ＩＣチップ１００に対する処理も含まれる。

【０１１４】プログラム制御部１１１は、外部インターフェース１０５経由で、ＩＣカード１００にアクセスすることができる。

【０１１５】また、プログラム制御部１１１には、情報格納部１１４が設けられている。情報格納部１１４は、例えばＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）のような書き込み可能なメモリ装置や、ハード・ディスクなどの外部記憶装置などで構成されている。

【０１１６】表示部１１２は、例えば液晶表示ディスプレイ（ＬＣＤ：liquid Crystal Display）で構成される。表示部１１２は、例えば、プログラム制御部１１１における処理結果などを画面出力してユーザに通知することができる。

【０１１７】ユーザ入力部１１３は、キーボードやジョグダイヤル、あるいは表示部１１２の表示画面に重畳されたタッチパネルなどで構成され、ユーザが携帯端末１１０にコマンドやデータを入力するために使用される。

【０１１８】携帯端末１１０内のプログラム制御部１１１は、バッテリなど図示しない主電源からの給電により駆動する。

【０１１９】ＩＣチップ１００を内蔵した携帯端末１１０をリーダ／ライタ（Ｒ／Ｗ）２００にかざすことによって、内蔵ＩＣチップ１００とリーダ／ライタ２００間で非接触データ通信が開始される。そして、ＰＩＮなどの暗証番号の照合を経て、ＩＣチップ１００内の電子チケットや電子マネーなどの価値情報へのアクセスが許可される。

【０１２０】［追補］以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１２１】

【発明の効果】以上詳記したように、本発明によれば、電子マネーや電子チケットなどの価値情報をセキュアに移動させることができる、優れたデータ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体を提供することができる。

【０１２２】また、本発明によれば、ＩＣカードやＩＣチップ内に保持されている電子マネーや電子チケットなどの価値情報をセキュアに移動させることができる、優れたデータ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体を提供することができる。

【０１２３】また、本発明によれば、ＩＣカードやＩＣチップ内に保持されている複数の価値情報を、１箇所のサーバに接続するだけでセキュアに移動させることができる、優れたデータ転送システム及びデータ転送方法、価値情報移動サービス装置及び価値情報移動サービス方法、並びに記憶媒体を提供することができる。

【０１２４】本発明によれば、移動用の価値情報のアクセス鍵と価値情報自体は、バリュー移動用サーバに保存する必要はなく、価値情報を運用するサービス・プロバイダのＳＡＭ内に保存される。したがって、価値情報の移動事業者と、価値情報サービスを運用する各サービス・プロバイダの責任範囲を明確に分離することができる。

【０１２５】また、本発明によれば、ＩＣチップ内の複数の価値情報を移動しなければならないような場合、価値情報の移動元ＩＣチップ、並びに、価値情報の移動先ＩＣチップのための各通信装置は、１箇所のバリュー移動用サーバのみと接続するだけで充分である。したがって、通信装置は手動又は自動で価値情報サービス毎に通信を逐次切り換える必要がない。このため、手間が減り、通信障害が起こる可能性を減少させることができる。この場合、ＩＣチップ側から考えると、１箇所のバリュー移動用サーバに接続すれば、中継先となる各サービス・プロバイダのＳＡＭの存在を意識する必要がない。

【０１２６】また、本発明によれば、移動前に価値情報へアクセスするための鍵を「仮鍵」に変更して、移動完了後に本鍵に戻すようにしているので、移動の途中で価値情報が不正に複製や改竄されて使用されることを防ぐことができる。また、価値情報の移動に失敗した場合であっても、移動元の鍵を本鍵に戻すことにより、価値情報の消失を防ぐことができる。

【図面の簡単な説明】

【図１】価値情報のセキュアな移動を実現するネットワーク・システムの構成を模式的に示した図である。

【図２】本実施形態に係るネットワーク・システム上におけるＩＣチップ間で価値情報をセキュアに移動させるための処理手順を示したフローチャートである。

【図３】移動元ＩＣチップに保持されている価値情報を個々のサービス・プロバイダの移動用ＳＡＭ１２にアップロードするための処理手続きを示したシーケンス図である。

【図４】個々のサービス・プロバイダの移動用ＳＡＭ１２にアップロードされている価値情報を移動元ＩＣチップにダウンロードするための処理手続きを示したシーケンス図である。

【図５】電磁誘導に基づくリーダ／ライタとＩＣカードとの無線通信の仕組みを概念的に示した図である。

【図６】リーダ／ライタとＩＣカードからなる系を１個のトランスとして捉えてモデル化した図である。

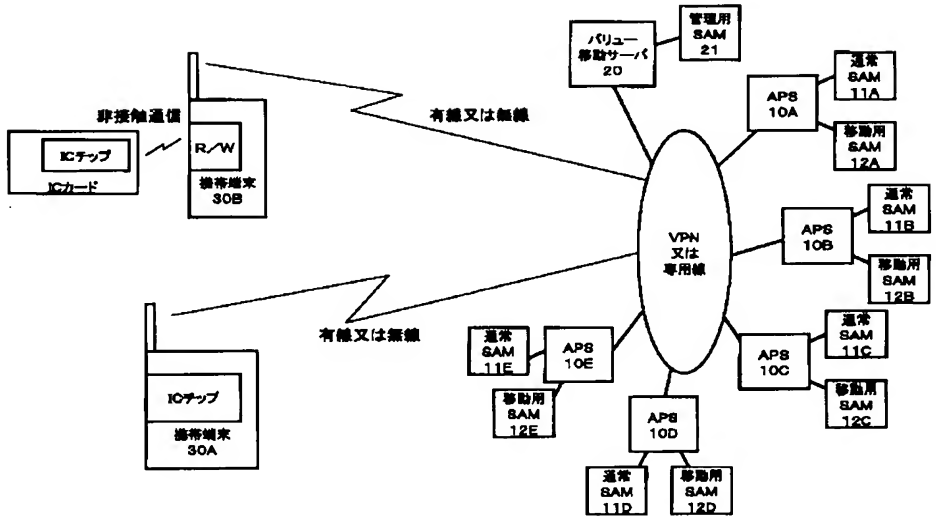
【図７】ＩＣチップ１００を内蔵したタイプの携帯端末１１０の内部ハードウェア構成を模式的に示した図である。

【符号の説明】

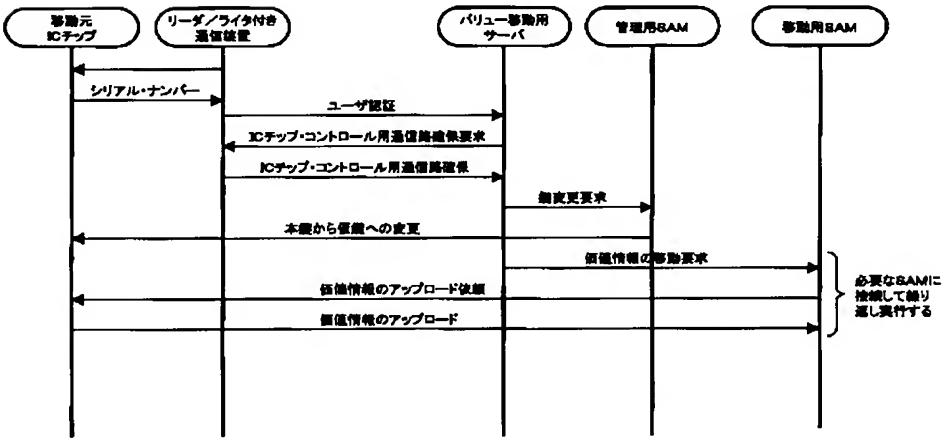
１０…アプリケーション・サーバ（サービス・プロバイダ）
１１…通常ＳＡＭ
１２…移動用ＳＡＭ
２０…バリュー移動用サーバ
２１…管理用ＳＡＭ
１００…ＩＣチップ
１０１…アンテナ部
１０２…アナログ部
１０３…ディジタル制御部
１０４…メモリ
１０５…外部インターフェース
１１０…携帯端末
１１２…表示部
１１３…ユーザ入力部

１１４…情報格納部　　２００…リーダ／ライタ

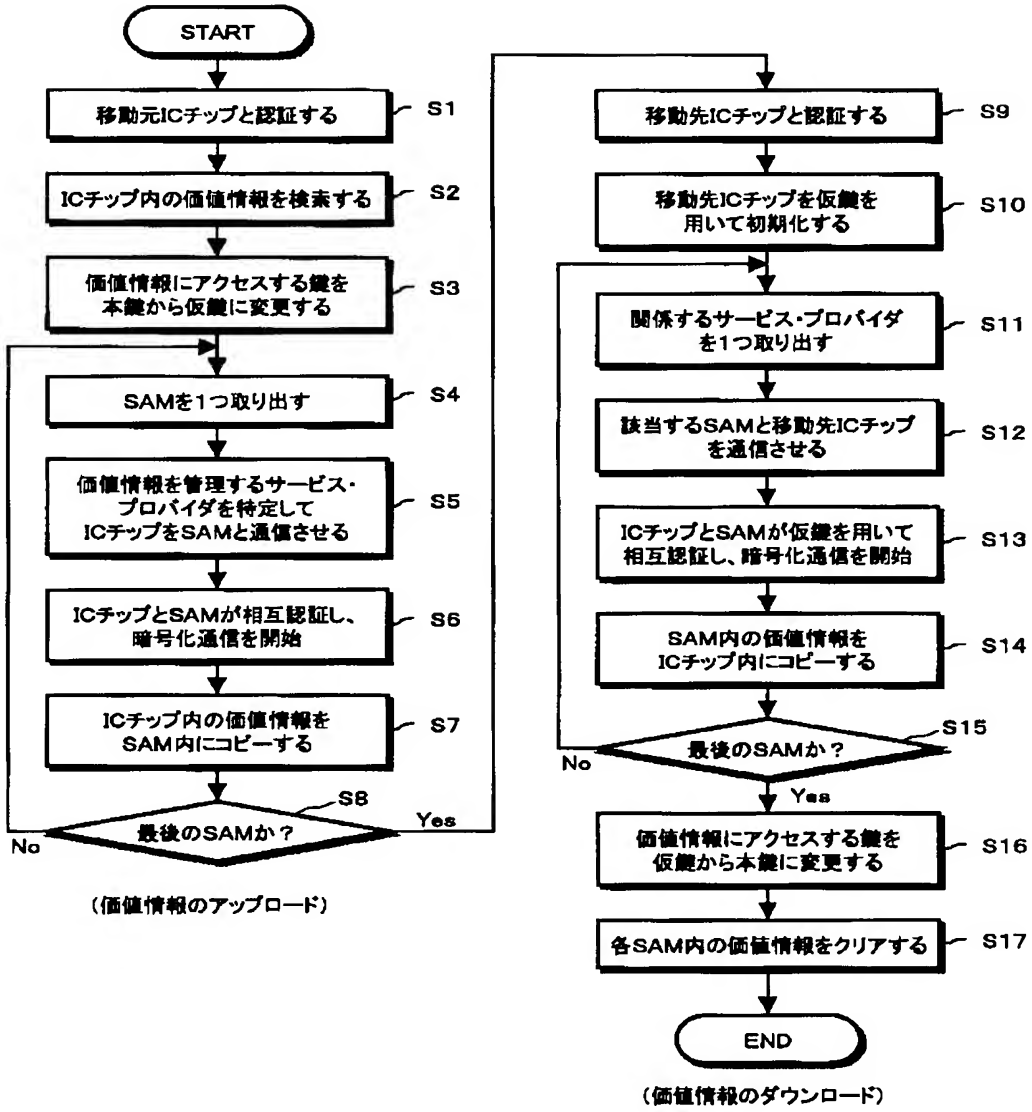
【図１】



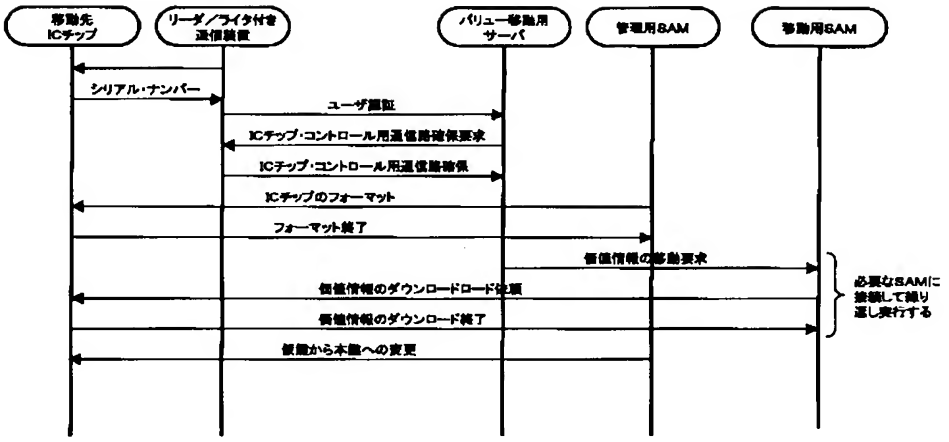
【図３】



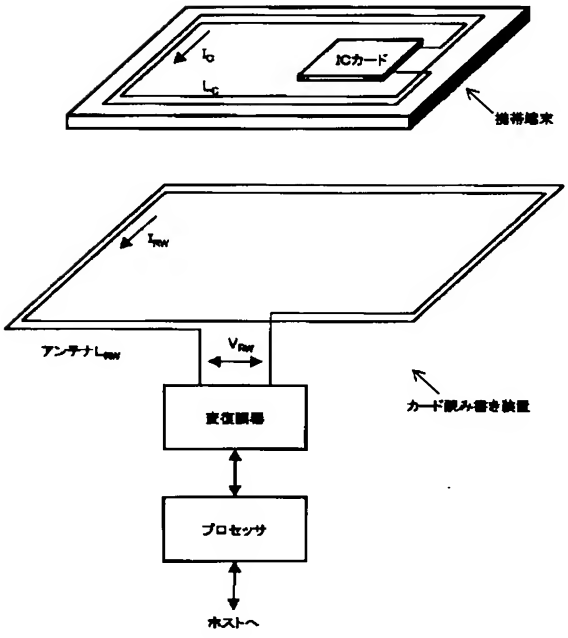
【図２】


START
移動元ICチップと認証する
S1
ICチップ内の価値情報を検索する
S2
価値情報にアクセスする鍵を本鍵から仮鍵に変更する
S3
SAMを1つ取り出す
S4
価値情報を管理するサービス・プロバイダを特定してICチップをSAMと通信させる
S5
ICチップとSAMが相互認証し、暗号化通信を開始
S6
ICチップ内の価値情報をSAM内にコピーする
S7
最後のSAMか？
S8
No
Yes
（価値情報のアップロード）
移動先ICチップと認証する
S9
移動先ICチップを仮鍵を用いて初期化する
S10
関係するサービス・プロバイダを1つ取り出す
S11
該当するSAMと移動先ICチップを通信させる
S12
ICチップとSAMが仮鍵を用いて相互認証し、暗号化通信を開始
S13
SAM内の価値情報をICチップ内にコピーする
S14
最後のSAMか？
S15
No
Yes
価値情報にアクセスする鍵を仮鍵から本鍵に変更する
S16
各SAM内の価値情報をクリアする
S17
END
（価値情報のダウンロード）

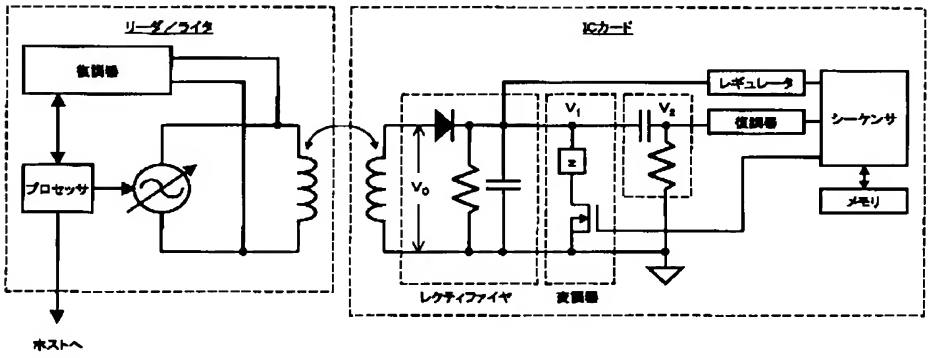
【図４】


移動先
ICチップ
リーダ／ライタ付き
通信装置
バリュー移動用
サーバ
管理用SAM
移動用SAM
シリアル・ナンバー
ユーザ認証
ICチップ・コントロール用通信路確保要求
ICチップ・コントロール用通信路確保
ICチップのフォーマット
フォーマット終了
価値情報の移動要求
価値情報のダウンロードロード依頼
価値情報のダウンロード終了
仮顧から本顧への変更
必要なSAMに
接続して繰り
返し実行する

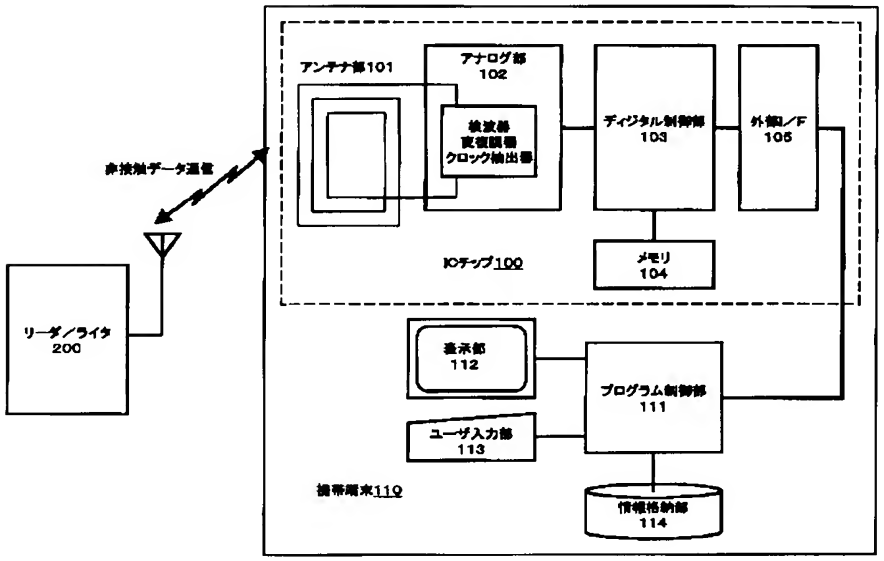
【図５】


ICカード
携帯端末
アンテナ
変復調器
プロセッサ
ホストへ
カード読み書き装置

【図６】


リーダ／ライタ
ICカード
復調器
プロセッサ
ホストへ
V_0
V_1
V_2
レギュレータ
復調器
シーケンサ
メモリ
レクティファイヤ
変調器

【図７】


アンテナ部101
アナログ部
102
検波器
変復調器
クロック抽出器
ディジタル制御部
103
外部I/F
105
非接触データ通信
ICチップ100
メモリ
104
リーダ／ライタ
200
表示部
112
プログラム制御部
111
ユーザ入力部
113
携帯端末110
情報格納部
114